AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

OVERSIGHT OF THE FEDERAL TRADE COMMISSION: STRENGTHENING PROTECTIONS FOR AMERICANS' PRIVACY AND DATA SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

MAY 8, 2019

Serial No. 116–31

Printed for the use of the Committee on Energy and Commerce
govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
40–157 PDF WASHINGTON : 2021

COMMITTEE ON ENERGY AND COMMERCE

FRANK PALLONE, JR., New Jersey
Chairman

BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
DIANA DEGETTE, Colorado
MIKE DOYLE, Pennsylvania
JAN SCHAKOWSKY, Illinois
G. K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJÁN, New Mexico
PAUL TONKO, New York
YVETTE D. CLARKE, New York, *Vice Chair*
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY III, Massachusetts
TONY CÁRDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan
MARC A. VEASEY, Texas
ANN M. KUSTER, New Hampshire
ROBIN L. KELLY, Illinois
NANETTE DIAZ BARRAGÁN, California
A. DONALD MCEACHIN, Virginia
LISA BLUNT ROCHESTER, Delaware
DARREN SOTO, Florida
TOM O'HALLERAN, Arizona

GREG WALDEN, Oregon
Ranking Member
FRED UPTON, Michigan
JOHN SHIMKUS, Illinois
MICHAEL C. BURGESS, Texas
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
TIM WALBERG, Michigan
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina
GREG GIANFORTE, Montana

PROFESSIONAL STAFF

JEFFREY C. CARROLL, *Staff Director*
TIFFANY GUARASCIO, *Deputy Staff Director*
MIKE BLOOMQUIST, *Minority Staff Director*

SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE

JAN SCHAKOWSKY, Illinois
Chairwoman

KATHY CASTOR, Florida
MARC A. VEASEY, Texas
ROBIN L. KELLY, Illinois
TOM O'HALLERAN, Arizona
BEN RAY LUJÁN, New Mexico
TONY CÁRDENAS, California, *Vice Chair*
LISA BLUNT ROCHESTER, Delaware
DARREN SOTO, Florida
BOBBY L. RUSH, Illinois
DORIS O. MATSUI, California
JERRY MCNERNEY, California
DEBBIE DINGELL, Michigan
FRANK PALLONE, JR., New Jersey *(ex officio)*

CATHY MCMORRIS RODGERS, Washington
Ranking Member
FRED UPTON, Michigan
MICHAEL C. BURGESS, Texas
ROBERT E. LATTA, Ohio
BRETT GUTHRIE, Kentucky
LARRY BUCSHON, Indiana
RICHARD HUDSON, North Carolina
EARL L. "BUDDY" CARTER, Georgia
GREG GIANFORTE, Montana
GREG WALDEN, Oregon *(ex officio)*

C O N T E N T S

	Page
Hon. Jan Schakowsky, a Representative in Congress from the State of Illinois, opening statement	1
Prepared statement	2
Hon. Cathy McMorris Rodgers, a Representative in Congress from the State of Washington, opening statement	4
Prepared statement	5
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	6
Prepared statement	8
Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement	9
Prepared statement	11

WITNESSES

Joseph J. Simons, Chairman, Federal Trade Commission	13
Prepared statement [1]	15
Answers to submitted questions	107
Christine S. Wilson, Commissioner, Federal Trade Commission	42
Answers to submitted questions	135
Rebecca Kelly Slaughter, Commissioner, Federal Trade Commission	43
Answers to submitted questions	143
Noah Joshua Phillips, Commissioner, Federal Trade Commission	45
Answers to submitted questions	151
Rohit Chopra, Commissioner, Federal Trade Commission	46
Answers to submitted questions	169

SUBMITTED MATERIAL

Letter of March 20, 2019, from Mr. Pallone and Ms. Schakowsky to Joseph J. Simons, Chairman, Federal Trade Commission, submitted by Ms. Schakowsky	85
Letter of April 1, 2019, from Joseph J. Simons, Chairman, Federal Trade Commission, to Ms. Schakowsky, submitted by Ms. Schakowsky	88
Letter of October 26, 2018, from James L. Madara, Executive Vice President and Chief Executive Officer, American Medical Association, to Joseph J. Simons, Chairman, Federal Trade Commission, submitted by Mr. Rush	93
Letter of May 6, 2019, from Marc Rotenberg, President, and Caitriona Fitzgerald, Policy Director, Electronic Privacy Information Center, to Ms. Schakowsky and Mrs. Rodgers, [2] submitted by Ms. Schakowsky	
Letter of May 8, 2019, from Richard Hunt, President and Chief Executive Officer, Consumer Bankers Association, to Mr. Pallone and Mr. Walden, submitted by Ms. Schakowsky	95

[1] Mr. Simons and the four FTC Commissioners submitted a joint prepared statement.

[2] The letter has been retained in committee files and also is available at https://docs.house.gov/meetings/IF/IF17/20190508/109415/HHRG-116-IF17-20190508-SD004.pdf.

Page

Letter of May 8, 2019, from Michael Beckerman, President and Chief Executive Officer, Internet Association, to Ms. Schakowsky and Mrs. Rodgers, submitted by Ms. Schakowsky 99

Letter of May 7, 2019, from Brad Thaler, Vice President of Legislative Affairs, National Association of Federally-Insured Credit Unions, to Ms. Schakowsky and Mrs. Rodgers, submitted by Ms. Schakowsky 101

Letter of May 8, 2019, from Tina Olson Grande, Healthcare Leadership Council, on behalf of the Confidentiality Coalition, Electronic Privacy Information Center, to Ms. Schakowsky and Mrs. Rodgers, submitted by Ms. Schakowsky 103

OVERSIGHT OF THE FEDERAL TRADE COMMISSION: STRENGTHENING PROTECTIONS FOR AMERICANS' PRIVACY AND DATA SECURITY

WEDNESDAY, MAY 8, 2019

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:30 a.m., in the John D. Dingell Room 2123, Rayburn Rayburn House Office Building, Hon. Jan Schakowsky (chairwoman of the subcommittee) presiding.

Members present: Representatives Schakowsky, Castor, Kelly, O'Halleran, Luján, Cárdenas, Blunt Rochester, Soto, Rush, Matsui, McNerney, Dingell, Pallone (ex officio), Rodgers (subcommittee ranking member), Upton, Burgess, Latta, Guthrie, Bucshon, Hudson, Carter, Gianforte, and Walden (ex officio).

Also present: Representative Walberg.

Staff present: Billy Benjamin, Systems Administrator; Jeffrey C. Carroll, Staff Director; Evan Gilbert, Deputy Press Secretary; Lisa Goldman, Senior Counsel; Waverly Gordon, Deputy Chief Counsel; Tiffany Guarascio, Deputy Staff Director; Alex Hoehn-Saric, Chief Counsel, Communications and Consumer Protection; Zach Kahan, Outreach and Member Service Coordinator; Meghan Mullon, Staff Assistant; Alivia Roberts, Press Assistant; Tim Robinson, Chief Counsel; Chloe Rodriguez, Policy Analyst; Ben Rossen, FTC Detailee; C. J. Young, Press Secretary; Jordan Davis, Minority Senior Advisor; Margaret Tucker Fogarty, Minority Staff Assistant; Melissa Froelich, Minority Chief Counsel, Consumer Protection and Commerce; Bijan Koohmaraie, Minority Counsel, Consumer Protection and Commerce; and Brannon Rains, Minority Legislative Clerk.

Ms. SCHAKOWSKY. The Subcommittee on Consumer Protection and Commerce will now come to order. We will begin with Member opening statements, and I will begin for 5 minutes.

OPENING STATEMENT OF HON. JAN SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

So, good morning, and thank you to the Federal Trade Commission for being with us this morning. It is really an honor to have all of you here. It means a great deal to us.

The FTC is an independent agency created by Congress to protect the American people. Recent media reports have focused on the Federal Trade Commission's potentially record-breaking fine of Facebook. The fact of the matter is that I believe that the public information known about this case underscores the need for comprehensive privacy legislation. And we are really going to focus, at least I am, on privacy legislation and what we can do.

And while I appreciate the Commission's work on and action on the Facebook case, I believe the reality is that a large fine in a single case does not meaningfully solve the problems that consumers face because of the FTC's lack of tools it needs to fulfill the mission to protect consumers in today's economy. The FTC needs increased funding and the APA, Administration Procedures Act—I can't stand those acronyms, OK—the rulemaking authority, at a minimum, to restore consumers' confidence in today's digital and brick-and-mortar marketplace, the FTC should be able to pursue multiple investigations both large and small.

And, Chairman Simons, I want to thank you and offer my support for APA rulemaking that you said that you wanted to see. We know the American people are counting on us to act. According to a recent survey, 67 percent of American adults want the Government to act to protect them and to protect their privacy. But as it stands right now, the FTC does not have authority to obtain civil penalties for initial violations for most unfair or deceptive practices, making matters much worse.

The Federal Trade Commission has only 40 full-time staff devoted to privacy and data security. Contrast that with the United Kingdom Information Commissioner's Office which has about 500 employees for a country about one-fifth of the size of the United States. And unfortunately, Chairman Simons, unlike other recent administrations, you have not appointed a chief technologist, and in fact only five people at the FTC right now are identified as technologists.

Energy and Commerce Democrats feel we have an obligation to provide a solid piece of legislation that protects consumer privacy. We have begun conversations now with the Republicans as well, and I am very hopeful that legislation will be bipartisan, and I am looking forward to working with all of you on the Federal Trade Commission in designing this legislation. We welcome the Commissioners today to learn how we can assist them in fulfilling their mission, our joint mission.

[The prepared statement of Ms. Schakowsky follows:]

PREPARED STATEMENT OF HON. JAN SCHAKOWSKY

I yield myself 5 minutes for an opening statement.

Good morning and thank you to the Federal Trade Commission for being here with us this morning. The FTC is an independent agency created by Congress to protect the American people.

Recent media reports have focused on FTC's potentially record-breaking fine of Facebook. The fact of the matter is that the public information known about that case underscores the need for comprehensive privacy legislation.

And while I appreciate the Commission's work and action on the Facebook case, I believe the reality is that a large fine in a single case does not meaningfully solve the problems consumers face because of the FTC's lack of tools it needs to fulfill the mission to protect consumers in today's economy.

The FTC needs increased funding and Administrative Procedure Act rulemaking authority at a minimum to restore consumer confidence in today's digital and brick-and-mortar marketplaces. The FTC should be pursuing multiple investigations, both large and small. Chairman Simons has publicly voiced support for Administration Proceedings Act rulemaking authority, and I am appreciative of those comments.

We know the American people are counting on us to act. According to a recent survey, 67 percent of American adults want the Government to act to protect their privacy.

But, as it stands, the FTC does not have authority to obtain civil penalties for initial violations for most unfair or deceptive practices. Making matters much worse, the FTC has only 40 full-time staff devoted to privacy and data security. Contrast that with the United Kingdom Information Commissioner's Office, which has about 500 employees for a country about one fifth the size of the United States. And unfortunately, Chairman Simons, unlike other recent administrations, has not appointed a Chief Technologist, and only 5 people at the FTC are technologists.

Energy and Commerce Democrats feel we have an obligation to produce a solid piece of legislation that protects consumer privacy. We've begun conversations now with the Republicans. It's my hope that this legislation will be bipartisan. And I am looking forward to working with the FTC in designing this legislation.

I welcome the Commission today to learn how we can assist them in fulfilling their mission.

Ms. SCHAKOWSKY. I want to yield the balance of my time to Congressman Luján.

Mr. LUJÁN. Thank you, Chairwoman Schakowsky. And I thank Chairman Pallone, Ranking Members Walden and Rodgers, for this important hearing today on privacy and data security.

Let me start with just a few numbers: 500 million, 148 million, and 87 million. These are the numbers of consumers impacted by the Marriott, 500 million; Equifax data breaches, 148 million; and the Facebook-Cambridge Analytica scandal, 87 million. These massive numbers represent real people, people whose trust and privacy has been violated. Most of them not been made whole, still vulnerable today.

Here is another number, 21. It has been 21 years since Congress passed even limited privacy legislation, the Children's Online Privacy Act. In 1998, America Online had 14 million subscribers, Google was a month old, and Facebook didn't even exist. These numbers make it real; we must act to pass comprehensive data privacy and security legislation.

And most recently in 2017, when we discovered and learned about the breach with Equifax back in September of '17, there were hearings held in October of '17. It appeared that there were commitments made in this committee to the American people that action would be taken before the holiday season and here we are today, still where no action taken and that is why this hearing matters so very much.

And so with that, Madam Chair, I thank you for the hearing. I urge us to act. And I thank the Commissioners for their testimony and I look forward to today's discussion. And I yield back.

Ms. SCHAKOWSKY. Would anyone else on the Democratic side want the time that is remaining? Otherwise, I yield back and I now recognize the ranking member, Ms. McMorris Rodgers, for her opening statement.

OPENING STATEMENT OF HON. CATHY McMORRIS RODGERS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WASHINGTON

Mrs. RODGERS. Thank you, Madam Chairman, and welcome to everyone, the Chairman and the Commissioners from the Federal Trade Commission.

Today's hearing is very important. Whether through deceptive advertising, fraud, or other schemes, bad actors regularly try to game the system and destroy trust. The FTC has been one of the top cops on the consumer protection beat for decades. I am glad that you are here to discuss the Commission's vital mission to protect consumers and promote competition and innovation especially as it relates to one of the most important issues today, our privacy.

In America's 21st century economy, our days start and end by exchanging our information with products that save us time, keep us informed, connect us with our communities. Many of us start our day by asking Alexa or Siri, "What is the weather today?" Then we browse Facebook and Instagram, open some emails, read the news, check for traffic updates on our iPhones, and if the traffic doesn't look too bad there is time to order groceries to be picked up or delivered after work. And that is just before we walk out the door. All day long, we are sharing our information with the internet marketplace. And for people who use health trackers and apps, it might not even stop when you go to sleep.

This free flow of information drives much of the innovation and technology growth here in the United States. Bottom line, we make choices every day to be connected, and when we do, we must be able to trust that our privacy is protected. We deserve to know how our data is being collected, how it is being used, and who it is being shared with. There shouldn't be so many surprises, and these protections shouldn't change depending upon which State we are in.

In a recent survey, 75 percent of respondents said privacy protections should be the same everywhere they go. The vast majority of Americans want the same protections whether they live in Eastern Washington, San Francisco, New Jersey, or Illinois. That is why I have been advocating and leading for a national standard for data privacy that, one, doesn't leave our privacy vulnerable in a patchwork; two, increases transparency and targets harmful practices like Cambridge Analytica; three, improves data security practices; and four, is workable for our Nation's innovators and small businesses.

So, today, I look forward to hearing from the Federal Trade Commission which is the main cop on the beat to enforce privacy standards, promote transparency, and hold companies accountable. The FTC's mission is to protect consumers and promote innovation. Our four principles for data privacy law are in line with the mission. It is about protecting consumers from concrete harms, empowering the choices that they make, and also promoting new technologies that we haven't even dreamed of yet. This Congress should lead on writing privacy rules of the road. I remain ready and willing to work with my colleagues on this committee for a bipartisan solution that puts consumers and their choices first.

In various proposals, some groups have called for the FTC to have additional resources and authorities. I remain skeptical of

Congress delegating broad authority to the FTC or any agency. However, we must be mindful of the complexities of this issue as well as the lessons learned from previous grants of rulemaking authority to the Commission.

The FTC's jurisdiction is incredibly broad. Its authority extends beyond just big tech, touching almost every aspect of our marketplace from loyalty programs at your local grocery store to your favorite coffee shop. The existing statutory rulemaking authority given to the FTC by Congress must also be part of the discussion. Had the FTC undertook rulemaking efforts on any number of issues we will discuss today, even starting 8 to 10 years ago, those efforts could have already been completed. The history of the FTC's authority is important, and it should not be transformed from a law enforcement agency to a massive rulemaking regime.

To understand the pain this could cause, look no further than GDPR in Europe. Investment in startups in Europe is down 40 percent and thousands of U.S. firms are no longer operating in the EU because they can't take on the millions of dollars in compliance cost. If we decide to increase FTC's resources and authority to enforce privacy law, then this committee must exercise its oversight of the Commission to its fullest. Oversight must be a part of the conversation, so Congress does its job to review and hold the FTC accountable.

Thank you, everyone, for being here, and I look forward to our discussion.

[The prepared statement of Mrs. Rodgers follows:]

PREPARED STATEMENT OF HON. CATHY MCMORRIS RODGERS

Good morning and welcome to the Consumer Protection and Commerce Subcommittee hearing with the Federal Trade Commission.

Thank you Chairman Simons, and Commissioners Phillips, Wilson, Chopra, and Slaughter.

Whether through deceptive advertising, fraud, or other schemes, bad actors regularly try to game our system. The FTC has been one of the top cops on the consumer protection beat for decades.

I'm glad you are here to discuss the Commission's vital mission to protect consumers and promote competition and innovation especially as it relates to one of the most important issues today—data privacy.

In America's 21st century economy, our days start and end by exchanging our information with products the save us time, keep us informed, and connect us with our communities.

Many of us start our days asking Alexa or Siri, what's the weather today? Then we browse Facebook and Instagram open some emails and read the news; check for traffic updates on our iPhones and if traffic doesn't look too bad, there's time to order groceries to be picked up or delivered after work.

And that's just before we walk out the door.

All day long we are sharing our information with the internet marketplace and for people who use health trackers and apps, it might not even stop when you go to sleep. This free flow of information drives much of the innovation and technology growth here in the U.S.

Bottom line, we make choices every day to be connected and when we do, we should be able to trust that our privacy is protected.

We deserve to know how our data is collected, how it's used, and who it's being shared with. There should be no surprises and these protections shouldn't change depending on what State we're in.

In recent survey, 75 percent of respondents said privacy protections should be the same everywhere they go. The vast majority of Americans want the same protections whether they are in Eastern Washington, San Francisco, New Jersey, or Illinois.

That's why we've been advocating and leading for a national standard for data privacy that:

One, doesn't leave our privacy vulnerable in a patchwork

Two, increases transparency and targets harmful practices, like Cambridge Analytica

Three, improves data security practices

And four, is workable for our Nation's innovators and small businesses.

So today, I look forward to hearing from the Federal Trade Commission which is the main cop on the beat to enforce privacy standards, promote transparency, and hold companies accountable.

The FTC's mission is to protect consumers and promote innovation. Our four principles for a data privacy law, are in line with that mission.

It's about protecting consumers from concrete harms, empowering the choices they make and also, promoting the new technologies that we haven't even dreamed of yet. This Congress should lead on writing the privacy rules of the road.

I remain ready and willing to work with my colleagues on the committee for a bipartisan solution that puts consumers and their choices first.

In various proposals some groups have called for the FTC to have additional resources and authorities. I remain skeptical of Congress delegating broad authority to the FTC or any agency, however we must be mindful of the complexities of these issues as well as the lessons learned from previous grants of rulemaking authority to the Commission.

The FTC's jurisdiction is incredibly broad. Its authority extends beyond just Big Tech, touching almost every aspect of our marketplace—from loyalty programs at your local grocery store to your favorite coffee shop.

The existing statutory rulemaking authority given to the FTC by Congress must also be part of this discussion. Had the FTC undertook rulemaking efforts on any number of issues we will discuss today. even starting 8 to 10 years ago. those efforts could have already been completed.

The history of the FTC's authority is important, and it should not be transformed from a law enforcement agency to a massive rulemaking regime. To understand the pain this could cause look no further than GDPR in Europe.

Investment in startups in Europe is down 40 percent and thousands of US firms are no longer operating in the EU because they can't take on the millions of dollars in compliance costs.

If we decide to increase the FTC's resources and authority to enforce a privacy law, then this committee must exercise its oversight of the Commission to its fullest extent.

Oversight must be part of this conversation. so Congress does its job to review and hold the FTC accountable.

Thank you all for being here today and I look forward to our discussion.

Ms. SCHAKOWSKY. The gentlelady yields back. And now I recognize the chair of the full committee, Mr. Pallone, for 5 minutes.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Madam Chair.

The Federal Trade Commission plays a critical role in protecting American consumers and promoting competition in the marketplace. It is a relatively small agency, but the breadth of its mission is vast. As the Nation's consumer protection agency, the FTC works to protect consumers from a variety of unfair and deceptive practices including false advertising, illegal telemarketing, unfair debt collection and fraud.

Last year, the FTC received nearly 3 million complaints from consumers who reported losing around $1½ billion to fraud. Seniors particularly were preyed upon by criminals pretending to need money to bail their grandchildren out of jail. Veterans were tricked into giving their credit card information to a thief who claimed to work for the Veterans Choice Program, just as examples. And these

two examples of the thousands of frauds the FTC face every day, many are perpetrated through robocalls which I am working to address through the Stopping Bad Robocalls Act.

But that is not the only way fraudsters commit their offenses and the FTC needs more support and more authority to prevent scams and enforce the law. The FTC is also the Nation's primary enforcer in the area of privacy and data security. Talk about a daunting job. When you consider that companies today monitor every move we make, they are tracking where we go, who we are with, our private conversations, our health, the websites we visit, and increasingly what we do inside our homes. And as we have learned from the concerning privacy issues surrounding Cambridge Analytica and Facebook and from massive data breaches like the one at Equifax, there is little reason to believe that consumers can trust these companies with our personal data.

The FTC can and should be doing more to protect consumers and Congress needs to give the FTC the tools it needs to be more effective. That starts with resources. The FTC has fewer employees today than it did in the 1980s when the internet did not exist. It has just 40 employees responsible for protecting the data of 300 million Americans. I think that is just unacceptable, particularly when you consider that the United Kingdom, which has a much smaller population, has more than 500 people who protect the privacy and data of its residents.

So we have to give the FTC the resources it needs to become a global leader on privacy and data security. The FTC also needs more authority to prevent privacy abuses from happening in the first place and to ensure that companies properly secure the personal data entrusted to them. Too often, the FTC can do little more than give a slap on the wrist to companies the first time they violate the law. That is because it lacks the authority to impose a monetary penalty for initial violations.

Currently, the FTC can only order a company to stop the bad practices and promise not to do it again. And if we really want to deter companies from breaking the law, the FTC needs to be able to impose substantial fines on companies the first time. To make matters worse, there are no strong and clear Federal privacy laws and regulations that establish a baseline for how companies collect, use, share, and protect consumer information. The FTC lacks the ability to issue such regulations, leaving Americans left to the whims of corporations.

Companies should not be gathering consumer information without a good reason and should have clear consent when they use that information for purposes a consumer would not reasonably expect. When I search online about the side effects of a medicine, I don't expect that information to be shared with advertisers, data brokers, or insurance companies, and it shouldn't be shared unless I say so.

Companies also need to protect the data they collect so Americans are not as vulnerable to identity theft, scams, and other unfair and deceptive acts as they are today. So Congress should pass, or must pass strong, comprehensive privacy legislation, and this committee intends to take that action. The legislation that we pass should give consumers control over their personal data including

giving consumers the ability to access, correct, and delete their personal information. And it should shift the burden to companies to ensure they only use the information consistent with reasonable consumer expectations.

So I look forward to hearing from all the Commissioners about how the FTC can better fulfill its mission in this important area of consumer protection.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

The Federal Trade Commission (FTC) plays a critical role in protecting American consumers and promoting competition in the marketplace. It is a relatively small agency, but the breadth of its mission is vast.

As the Nation's consumer protection agency, the FTC works to protect consumers from a variety of unfair and deceptive practices, including false advertising, illegal telemarketing, unfair debt collection, and fraud.

Last year, the FTC received nearly 3 million complaints from consumers who reported losing around $1.5 billion to fraud. Seniors were preyed upon by criminals pretending to need money to bail their grandchildren out of jail. Veterans were tricked into giving their credit card information to a thief who claimed to work for the Veterans Choice Program.

These are just two examples of the thousands of frauds the FTC faces every day. Many are perpetrated through robocalls, which I am working to address through the Stopping Bad Robocalls Act. But that is not the only way fraudsters commit their offences and the FTC needs more support and more authority to prevent scams and enforce the law.

The FTC is also the Nation's primary enforcer in the area of privacy and data security. Talk about a daunting job when you consider that companies today monitor every move we make. They are tracking where we go, who we are with, our private conversations, our health, the websites we visit, and, increasingly, what we do inside our homes. As we have learned from the concerning privacy issues surrounding Cambridge Analytica and Facebook, and from massive data breaches like the one at Equifax, there is little reason to believe that consumers can trust these companies with our personal data.

The FTC can and should be doing more to protect consumers, and Congress needs to give the FTC the tools it needs to be more effective. That starts with resources. The FTC has fewer employees today than it did in the 1980s when the Internet did not exist. It has just 40 employees responsible for protecting the data of 300 million Americans. That's unacceptable—particularly when you consider that the United Kingdom, which has a much smaller population, has more than 500 people who protect the privacy and data of its residents. We must give the FTC the resources it needs to become a global leader on privacy and data security.

The FTC also needs more authority to prevent privacy abuses from happening in the first place and to ensure that companies properly secure the personal data entrusted to them.

Too often, the FTC can do little more than give a slap on the wrist to companies the first time they violate the law. That's because it lacks the authority to impose a monetary penalty for initial violations. Currently, the FTC can only order a company to stop the bad practices and promise not to do it again. If we really want to deter companies from breaking the law, the FTC needs to be able to impose substantial fines on companies the first time.

To make matters worse, there are no strong and clear Federal privacy laws and regulations that establish a baseline for how companies collect, use, share, and protect consumer information. The FTC lacks the ability to issue such regulations leaving Americans left to the whims of corporations.

Companies should not be gathering consumer information without a good reason and should have clear consent when they use that information for purposes a consumer would not reasonably expect. When I search online about the side effects of a medicine, I don't expect that information to be shared with advertisers, data brokers, or insurance companies and it shouldn't be shared unless I say so. Companies also need to protect the data they collect so Americans are not as vulnerable to identity theft, scams, and other unfair and deceptive acts as they are today.

Congress must pass strong, comprehensive privacy legislation, and this committee will take action. The legislation should give consumers control over their personal data, including giving consumers the ability to access, correct, and delete their per-

sonal information. And it should shift the burden to companies to ensure they only use the information consistent with reasonable consumer expectations.

I look forward to hearing from all of the Commissioners about how the FTC can better fulfill its mission in this important area of consumer protection. Thank you, and I yield back my time.

Mr. PALLONE. And unless somebody wants the time, there is not much left—yes, I will yield to the gentlewoman from Florida.

Ms. CASTOR. Well, I thank the chairman of the committee for yielding the time.

And I just wanted to start out by saying that America needs a modern online privacy law and the Federal Trade Commission needs the tools and resources to effectively enforce law and hold bad actors accountable. And I think, I encourage you all today to also discuss the Children's Online Privacy Protection Act because I think it is in need of substantial updates, especially looking at how we enforce it, the sham safe harbor provisions, and your opinions on adopting some reasonable collection parameters. So thank you, and I yield back.

Mr. PALLONE. And I yield back, Madam Chair.

Ms. SCHAKOWSKY. The gentleman yields back, and now I will recognize the ranking member of the committee, Mr. Walden, for 5 minutes.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. Good morning, Madam Chair. Thanks for having this hearing. I want to welcome our Commissioners as well for being here from the Federal Trade Commission. Thank you. We will be informed by your testimony and we appreciate the work you do at the FTC.

We know you're tasked with broad and important responsibilities and it is a jurisdiction that spreads out over almost every aspect of the United States economy from large household name technology companies at Silicon Valley to small mom and pop shops in rural America. But recently concerns surrounding data security and data privacy including questions about what information is collected, how companies use that information, who that information is shared with, and what protections exist for consumers have demanded more and more congressional attention and appropriately so.

In the last Congress, this committee held very high-profile hearings around incidents involving data security and data privacy issues with CEOs. They sat right there from Equifax; Mark Zuckerberg was there for 5 hours from Facebook; we had those from Twitter as well. We also held hearings focused on securing consumer information, on understanding algorithmic decision making, exploring the online advertising ecosystem and how it operates, and an oversight hearing with you, the FTC. Privacy was a premier issue during these hearings, but as we learned, this is also a tough issue to legislate on. Privacy does not mean the exact same thing to each and every person.

I want to echo the sentiments of my colleague, Representative Rodgers, who outlined the vast benefits consumers also get from the use of their information online. It is a goods for services ex-

change. We don't always know that but we do benefit from that. We cannot lose sight of the tremendous benefits consumers get from the use of this data: access to top-tier journalism, affordable and quickly delivered products, telehealth and research initiatives, and much, much more.

Here in the United States we have a thriving startup ecosystem and a regulatory environment that enables small businesses to grow and compete in no small part because the free flow of information. And as a result, companies innovate, they create jobs in America, and offer consumers options and convenience that most of us never dreamed would be possible.

I believe it is important we work together toward a bipartisan, Federal privacy bill and we are ready and willing to tackle crafting such a bill. I think we were informed by our hearings in the last 2 years and are more than prepared now to move forward to write legislation in a bipartisan way. A Federal privacy bill must set one national standard. Allowing a patchwork of State laws will not only hurt innovation and small businesses, but will limit consumers' options online. Consumers expect a seamless online experience and I do not want to see that taken away.

We must protect innovation and small businesses. We should learn from Europe where large companies are only getting larger and unfortunately small companies are getting smaller or disappearing altogether online. You know, JPMorgan Chase & Company CEO Jamie Dimon recently said Dodd-Frank created a moat around his company, which is exactly what we risk doing with the likes of Google and Facebook and the big ones, because they will always be able to comply, and they will just get bigger if we don't craft the law correctly.

We must enhance security for consumers. Companies must have reasonable practices in place to protect consumer information, period. We must increase transparency. Consumers deserve to know how their information is collected, how it is used, and how it is shared. And we must improve accountability. When companies fail to keep their promises or outright misuse consumer information, those companies must be held accountable. This goes to the heart of the enforcement issues. Federal Trade Commission accomplishes its consumer protection mission through law enforcement, by bringing action against companies who engage in unfair or deceptive acts or practices. And we know you have a big decision before you right now involving one of those companies.

Through advocacy, through consumer and business education efforts, you do it all. The FTC can file injunctions, you can levy civil penalties, and you can seek remedies on behalf of consumers to redress harms. The Federal Trade Commission generally operates a highly effective, bipartisan agency, returning millions directly to consumers after they are defrauded, and I look forward to hearing an update on those efforts. I also look forward to hearing about the consumer protection hearings and what the agency has learned about privacy harms and risks.

Every agency has challenges and recent court changes in cases have changed the direction of some agency activity to refocus on due process. I am encouraged that these types of improvements would help small businesses understand their rights when faced

with the full force of the FTC. I believe the FTC is the right agency to enforce new privacy law with appropriate safeguards and process improvements to ensure strong, consistent enforcement.

Some have suggested the quick answer is more money, more rulemaking authority, and more employees. There is no quick fix, I would argue. I would like to hear from the Chairman about his views on unbounded rulemaking at the FTC and whether the agency can compete for talent with the big tech companies that are moving to the DC area. And we must consider market realities and ask if there are more effective ways to get experts to the FTC for unique cases.

So, Madam Chair, thanks for having this hearing. I think it is really important and we look forward to working with you and others on the committee to get this right and get it into law. And I yield back.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Good morning. I want to thank Chairman Simons and Commissioners Phillips, Wilson, Chopra, and Slaughter for being here. I am glad to see the five of you here again after our productive conversation last summer before this subcommittee.

The Federal Trade Commission is tasked with broad and important responsibilities and its jurisdiction spreads out over almost every aspect of the U.S. economy—from large, household-named technology companies in Silicon Valley to small mom-and-pop shops in rural America.

But, recently, concerns surrounding data security and data privacy, including questions about what information is collected, how companies use that information, who that information is shared with, and what protections exist for consumers, have demanded more Congressional attention.

Last Congress, this committee held high-profile hearings around incidents involving data security and data privacy issues with the CEOs of Equifax, Facebook, and Twitter. We also held hearings focused on: securing consumer information; understanding algorithmic decision making; exploring the online advertisement ecosystem and how it operates; and an oversight hearing with you, the FTC.

Privacy was a premiere issue during these hearings. But as we learned, this is a tough issue; privacy does not mean the exact same thing to every American.

I want to echo the sentiments of my colleague Rep. Rodgers who outlined the vast benefits consumers get from the use of their information online. We cannot lose sight of the tremendous benefits consumers get from the use of data—access to top-tier journalism, affordable and quickly delivered products, telehealth and research initiatives, and much more.

Here in the U.S., we have a thriving startup ecosystem and a regulatory environment that enables small businesses to grow and compete, in no small part because of the free flow of information. And, as a result, companies innovate, create new jobs, and offer consumers options and convenience.

I believe it is important that we work together toward a bipartisan Federal privacy bill. And we are ready and willing to tackle crafting such a bill. I hope that we can continue down the bipartisan path together.

A Federal privacy bill must set one national standard. Allowing a patchwork of State laws will not only hurt innovation and small businesses but will limit consumers options online. Consumers expect a seamless online experience, and I do not want to see that taken away.

We must protect innovation and small businesses. We should learn from Europe—where large companies are only getting larger and small companies are only getting smaller. JPMorgan Chase & Co. CEO Jamie Dimon recently said Dodd-Frank created a moat around his company—which is exactly what we risk doing with the likes of Google and Facebook if we do not carefully craft a national privacy bill.

We must enhance security for consumers. Companies must have reasonable practices in place to protect consumer information.

We must increase transparency—consumers deserve to know how their information is collected, used, and shared.

And we must improve accountability. When companies fail to keep their promises or outright misuse consumer information, those companies must be held accountable. This goes to the heart of the enforcement issues.

The FTC accomplishes its consumer protection mission through law enforcement—by bringing actions against companies who engage in unfair or deceptive acts or practices; through advocacy; and through consumer and business education efforts. The FTC can file injunctions, levy civil penalties, and can seek remedies on behalf of consumers to redress their harms.

The FTC generally operates as a highly effective bipartisan agency. Returning millions directly to consumers after they are defrauded, and I look forward to hearing an update on those efforts. I also look forward to hearing about the consumer protection hearings and what the agency has learned about privacy harms and risks.

Every agency has challenges, and recent court cases have changed the direction of some agency activity to refocus on due process. I am encouraged that these types of improvements would help small businesses understand their rights when faced with the full force of the FTC.

I believe the FTC is the right agency to enforce a new privacy law with appropriate safeguards and process improvements to ensure strong, consistent enforcement. Some have suggested that the quick answer is more money, more rulemaking authority, and more employees. There is no quick fix. I would like to hear from the Chairman about his views on unbounded rulemaking for the FTC, and whether the agency can compete for talent with the big tech firms moving to the DC area. We must consider market realities and ask if there is a more effective way to get experts to the FTC for unique cases.

I look forward to hearing from you all about how you are thinking of using the current tools at the FTC to address privacy concerns in our digital world.

Thank you.

Ms. SCHAKOWSKY. The gentleman yields back. And the Chair would like to remind Members that, pursuant to committee rules, all Members' written opening statements shall be made part of the record.

Next, I am going to introduce all of our witnesses, but I want to tell all of you that I had a standing-room-only FTC-sponsored scam workshop in my district along with Congressman Brad Schneider, which was amazing, and I would encourage all Members to consider doing that. The turnout was unprecedented, and people really appreciated it. So thank you.

So let me introduce our witnesses. The Honorable Joseph Simons, Chairman of the Federal Trade Commission; Commissioner Christine Wilson; Honorable Commissioner Rebecca Kelly—Rebecca Kelly Slaughter, sorry; Commissioner Noah Joshua Phillips; Commissioner Rohit Chopra. We are happy to have you all, and we want to thank our witnesses for joining us today. We look forward to your testimony.

And at this time, the Chair will now recognize each witness for 5 minutes to provide their opening statements.

Before we begin, I would like to explain the lighting system. I think probably most of you know that the light will initially be green at the start of your opening statement, then it will go to yellow when you have 1 minute, and then it will go to red. And we would appreciate it very much if you would end in those 5 minutes. So, Chairman Simons, you are recognized for your 5 minutes.

STATEMENTS OF JOSEPH J. SIMONS, CHAIRMAN, AND CHRISTINE S. WILSON, REBECCA KELLY SLAUGHTER, NOAH JOSHUA PHILLIPS, AND ROHIT CHOPRA, COMMISSIONERS, FEDERAL TRADE COMMISSION

STATEMENT OF JOSEPH J. SIMONS

Mr. SIMONS. Chairman Schakowsky, Ranking Member Rodgers, and distinguished members of the subcommittee, it is an honor and a privilege to appear before you today, and especially with my esteemed colleagues, my fellow Commissioners.

The FTC is a highly effective, independent agency with a broad mission to protect consumers and maintain competition in most sectors of the economy. On the competition side, examples of our vigorous enforcement program include cases like Impax and AbbVie where we successfully attacked anticompetitive conduct by pharmaceutical companies.

Ms. SCHAKOWSKY. If you could hold just for a minute.

We got the message, and if you will put the signs down, appreciate it.

Thank you. Go ahead.

Mr. SIMONS. Yes. We successfully attacked anticompetitive conduct by pharmaceutical companies, achieving a $448 million judgment in the latter case. We also recently filed an important case against a company called Surescripts, a health IT company with a monopoly over e-prescribing that is maintaining and acquired that monopoly through exclusionary conduct.

And on the research and policy front, our extensive Hearings on Competition and Consumer Protection in the 21st Century have involved more than 350 panelists and more than 850 public comments. On the consumer protection side, we are very active as well, with matters ranging from student debt relief scams to various types of false advertising and many other cases in between.

But today I would like to focus my remarks on data security and privacy. As you have said, the FTC has been the primary Federal agency charged with protecting consumer privacy since 1970 with the passage of the FCRA. From the growth of the internet to the mobile device explosion to the arrival of the Internet of Things and artificial intelligence, we have continuously expanded our focus on privacy to reflect how consumer data fuels these changes in the marketplace.

Our primary legal authority in this space is Section 5 of the FTC Act, which prohibits deceptive or unfair commercial practices. But Section 5 is an imperfect tool—imperfect tool. For example, Section 5 does not allow the Commission to seek civil penalties for first-time privacy violations. It does not allow us to reach nonprofits and common carriers even when their practices have serious implications for consumer privacy and data security.

These limitations have a critical effect on our ability to protect consumers, which is why we urge Congress to enact privacy and data security legislation enforceable by the FTC which grants the FTC civil penalty authority, targeted APA rulemaking authority, and jurisdiction over nonprofits and common carriers. Irrespective of any new legislation, however, we will continue to use every tool currently at our disposal to address consumer harm including au-

thorities given to us by the Congress like the Children's Online Privacy Protection Act and the Safeguards Rule.

We have aggressively pursued privacy and data security cases to date bringing more than 65 data security cases as well as more than 60 general privacy cases. For example, we recently brought cases against two companies whose alleged lax security practices resulted in a breach of 8 million consumers' data. And in March, the FTC announced a record $5.7 million civil penalty as part of its settlement with video social networking app Musical.ly for collecting children's personal information online without first obtaining parental consent.

To complement our efforts, we also engage in policy initiatives in the privacy and data security areas. In addition to the hearings I mentioned, which included 4 days of panels that specifically addressed consumer privacy and data security, we recently issued 6(b) orders to several internet service providers to evaluate their privacy practices. We will use the information we learned from this study to better inform our policy and our enforcement work.

Finally, many of our privacy and data security investigations in cases involve complex facts and technologies and well-financed defendants. And as we told you in response to Chairman Pallone and Schakowsky's resource letter, it is critical that the FTC have sufficient resources to support its investigative and litigation needs particularly as demand for enforcement in this area continues to grow. We are committed to using every resource effectively to protect consumers and to promote competition, to anticipate and respond to changes in the marketplace, and to meet current and future challenges.

We look forward to working with the subcommittee and the Congress and I am very happy to answer your questions. Thank you so much.

[The joint prepared statement of Mr. Simons and the four Commissioners follows:]

PREPARED STATEMENT OF THE

FEDERAL TRADE COMMISSION:

OVERSIGHT OF THE FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE

UNITED STATES HOUSE OF REPRESENTATIVES

WASHINGTON, DC

MAY 8, 2019

I. INTRODUCTION

Chairwoman Schakowsky, Ranking Member McMorris Rodgers, and members of the Subcommittee, the Federal Trade Commission ("FTC" or "Commission") is pleased to appear before you today to discuss the FTC's work to protect consumers and promote competition.[1]

The FTC is an independent agency with three main bureaus: the Bureau of Consumer Protection ("BCP"); the Bureau of Competition ("BC"); and the Bureau of Economics ("BE"), which supports both BCP and BC. The FTC is the only federal agency with a broad mission to both protect consumers and maintain competition in most sectors of the economy. Our jurisdiction includes privacy and data security, consumer fraud, mergers and acquisitions, and anticompetitive tactics by pharmaceutical and other companies. We enforce the law across a range of sectors, including health care, high technology, and emerging industries. The FTC has a long history of bipartisanship and cooperation, and we work hard to maintain it.

The FTC has broad law enforcement responsibilities under the Federal Trade Commission Act,[2] and enforces a wide variety of other laws, ranging from the Clayton Act to the Fair Credit Reporting Act. In total, the Commission has enforcement or other responsibilities under more than 75 laws.[3] The Commission pursues a vigorous and effective law enforcement program, and the impact of its work is significant. Its competition enforcement program is critically important to maintaining competitive markets across the country: vigorous competition results in lower prices, higher quality goods and services, and innovative and beneficial new products and services.

---

[1] This written statement presents the views of the Federal Trade Commission. The oral statements and responses to questions reflect the views of individual Commissioners, and do not necessarily reflect the views of the Commission or any other Commissioner.
[2] 15 U.S.C. § 41 *et seq.*
[3] *See* https://www.ftc.gov/enforcement/statutes.

The FTC also investigates and prosecutes those engaging in unfair or deceptive acts or practices, and seeks to do so without impeding lawful business activity. The agency has a varied toolkit to advance its mission. For example, the Commission collects consumer complaints from the public and maintains one of the most extensive consumer protection complaint databases, Consumer Sentinel. The FTC and other federal, state, and local law enforcement agencies use these complaints in their law enforcement and policy efforts. The FTC also has rulemaking authority. In addition to the FTC's Magnuson-Moss rulemaking authority, Congress has given the agency discrete rulemaking authority under the Administrative Procedure Act ("APA") over specific topics. The agency regularly analyzes its rules, including seeking public feedback, to ensure their continued efficacy. The FTC also educates consumers and businesses to encourage informed consumer choices, compliance with the law, and public understanding of the competitive process.

To complement these enforcement and public education efforts, the FTC pursues a consumer protection and competition policy and research agenda to improve agency decision-making, and engages in advocacy and education initiatives. Last fall, the Commission began its *Hearings on Competition and Consumer Protection in the 21st Century*.[4] This extensive series of public hearings is exploring whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection law, enforcement priorities, and policy. To date, we have heard from more than 350 panelists and received more than 850 public comments. The formal hearings will conclude shortly, and we will be accepting public comments through at least the end

[4] FTC, *Hearings on Competition and Consumer Protection in the 21st Century*, https://www.ftc.gov/policy/hearings-competition-consumer-protection; *see also* FTC Press Release, *FTC Announces Hearings On Competition and Consumer Protection in the 21st Century* (June 20, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st.

of June. These hearings underscore the unique role that the FTC plays in the development of sound competition and consumer protection policy.

This testimony discusses the FTC's work to protect U.S. consumers and competition, including highlights of some of the agency's major recent activities and initiatives. It also discusses the Commission's international efforts to protect consumers and promote competition.

II. CONSUMER PROTECTION MISSION

As the nation's primary consumer protection agency, the FTC has a broad mandate to protect consumers from unfair and deceptive practices in the marketplace, including fraud. We do this by, among other things, pursuing law enforcement actions to stop and deter unlawful practices, and educating consumers and businesses about their rights and responsibilities. The FTC's enforcement and education efforts include working closely with federal, state, international, and private sector partners on joint initiatives. Among other issues, the FTC works to protect privacy and data security, helps ensure that advertising claims to consumers are truthful and not misleading, addresses fraud across most sectors of the economy, and combats illegal robocalls.

The FTC's law enforcement orders prohibit defendants from engaging in further illegal activity, impose other compliance obligations, and in some cases, ban defendants from engaging in certain conduct altogether. Where appropriate, the FTC collects money to return to harmed consumers. During FY 2018, Commission actions resulted in over $1.6 billion being returned to consumers. Specifically, the Commission returned more than $83.3 million in redress to consumers, and the FTC resolved matters—including in the *Volkswagen*,[5] *Amazon*,[6] and

[5] *FTC v. Volkswagen Group of America, Inc.*, No. 3:15-md-02672-CRB (N.D. Cal. May 17, 2017), https://www.ftc.gov/enforcement/cases-proceedings/162-3006/volkswagen-group-america-inc.
[6] *FTC v. Amazon.com, Inc.*, No. 2:14-cv-01038 (W.D. Wash. Apr. 4, 2017), https://www.ftc.gov/enforcement/cases-proceedings/122-3238/amazoncom-inc.

NetSpend[7] matters—that required defendants to self-administer consumer refund programs worth more than $1.6 billion. The FTC also collected civil penalties worth more than $2.4 million and forwarded an additional $8.5 million to the U.S. Treasury in FY 2018.

A. Protecting Consumer Privacy and Data Security

Since the enactment of the Fair Credit Reporting Act ("FCRA")[8] in 1970, the FTC has served as the chief federal agency charged with protecting consumer privacy. With the development of the internet as a commercial medium in the 1990s, the FTC expanded its focus on privacy to reflect the growing collection, use, and sharing of consumer data in the commercial marketplace.

The Commission's primary source of legal authority in the privacy and data security space is Section 5 of the FTC Act, which prohibits deceptive or unfair commercial practices.[9] Under Section 5 and other authorities granted by Congress, the FTC has aggressively pursued privacy and data security cases in myriad areas, including children's privacy, financial privacy, health privacy, and the Internet of Things.[10] To date, the Commission has brought more than 65 cases alleging that companies failed to implement reasonable data security safeguards, and more than 60 general privacy cases.[11]

Section 5, however, is not without its limitations. For example, Section 5 does not allow the Commission to seek civil penalties for the first offense. It also excludes non-profits and common

---

[7] *FTC v. NetSpend Corp.*, No. 1:16-cv-04203-AT (N.D. Ga. Apr. 10, 2017), https://www.ftc.gov/enforcement/cases-proceedings/netspend-corporation.

[8] 15 U.S.C. § 1681. Among other things, the FCRA prohibits the unauthorized disclosure of sensitive data used for credit, employment, and other decisions

[9] 15 U.S.C. § 45. The Commission also enforces sector-specific statutes containing privacy and data security provisions, such as the Gramm-Leach-Bliley Act ("GLB Act"), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.), and the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6506.

[10] *See, e.g.*, FTC, PRIVACY & DATA SECURITY UPDATE: 2017 (Jan. 2018), https://www.ftc.gov/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives.*Id.*

[11] *Id.*

carriers from the Commission's authority, even when the acts or practices of these market participants have serious implications for consumer privacy and data security. To better equip the Commission to meet its statutory mission to protect consumers, we urge Congress to enact privacy and data security legislation, enforceable by the FTC, which grants the agency civil penalty authority, targeted APA rulemaking authority, and jurisdiction over non-profits and common carriers.[12]

While the Commission believes new authority could be very beneficial for American consumers, we also will continue to use every tool currently at our disposal to address consumer harm. For example, the Commission protects children's privacy online by enforcing the Children's Online Privacy Protection Act (COPPA). We recently alleged that Unixiz, doing business as i-Dressup.com, violated the COPPA Rule by failing to obtain parental consent prior to collecting personal information from children, as well as failing to protect children's personal information.[13] The FTC's complaint also alleged that the company stored and transmitted users' personal information in plain text, failed to implement an intrusion detection and prevention system, and failed to monitor for potential security incidents. As a result, a hacker accessed the personal information of approximately 2.1 million users, including 245,000 users under the age of 13. And in March, the FTC announced a settlement with the operators of the popular video social networking app Musical.ly, now known as Tik Tok, for COPPA violations.[14] The FTC alleged that the company collected children's personal information online without first obtaining parental

[12] Commissioner Phillips supports congressional efforts to consider consumer data privacy legislation. He believes legislation should be based on harms that Congress agrees warrant a remedy, and that tools like penalties and rulemaking should be calibrated carefully to address those harms. Commissioner Phillips believes Congress should also give appropriate consideration to the trade-offs involved in new regulation, and, with regard to rulemaking, reserve to itself fundamental value judgments appropriately made by the legislature. Finally, Commissioner Phillips believes data security legislation is a critical step Congress should also take to protect consumer privacy.
[13] *U.S. v. Unixiz, Inc. d/b/a i-Dressup.com et al.*, No. 5:19-cv-02222 (N.D. Cal. Apr. 24, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3002/unixiz-inc-doing-business-i-dressupcom.
[14] *U.S. v. Musical.ly, et al.*, No. 2:19-cv-1439 (C.D. Ca. Mar. 27, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3004/musically-inc.

consent. Because COPPA allows the Commission to seek civil penalties for its violations, the defendants agreed to pay a $5.7 million dollar civil penalty, the largest ever obtained by the Commission in a COPPA case.

Further examples of data security enforcement include the Commission's settlement with Uber Technologies over the company's alleged failure to reasonably secure sensitive consumer data stored in the cloud.[15] As a result, an intruder allegedly accessed personal information about Uber customers and drivers, including more than 25 million names and email addresses, 22 million names and mobile phone numbers, and 600,000 names and driver's license numbers. Uber suffered a second, larger breach of drivers' and riders' data in October-November 2016, and failed to disclose that breach to consumers or the FTC for more than a year, despite being the subject of an ongoing FTC investigation of its data security practices during that time. Among other things, the final order prohibits Uber from misrepresenting how it monitors internal access to consumers' personal information and the extent to which it protects personal information, with the threat of strong civil penalties if it fails to comply.[16] And in May 2018, the Commission resolved allegations that PayPal's Venmo peer-to-peer payment service misled consumers about their ability to control the privacy of their Venmo transactions and the extent to which their financial accounts were protected by "bank grade security systems."[17]

Just this past month, the Commission settled with an online rewards website, Clixsense.com, for its alleged failure to take appropriate steps to secure consumers' data.[18] The FTC alleged that

---

[15] *See* FTC Press Release, *Federal Trade Commission Gives Final Approval to Settlement with Uber* (Oct. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/federal-trade-commission-gives-final-approval-settlement-uber.

[16] As discussed above, because the FTC does not have civil penalty authority under Section 5, it could not require Uber to pay a civil penalty in the first instance.

[17] *PayPal, Inc.*, No. C-4651 (May 24, 2018), https://www.ftc.gov/enforcement/cases-proceedings/162-3102/paypal-inc-matter.

[18] *James. V. Grago, Jr. also d/b/a ClixSense.com*, Matter No. 1723003 (Apr. 24, 2019) (proposed consent order), https://www.ftc.gov/enforcement/cases-proceedings/172-3003/james-v-grago-jr-doing-business-clixsensecom.

the company's inadequate security—including its storage of personal information in plain text and its failure to perform vulnerability and penetration testing—allowed hackers to gain access to the company's network through a browser extension downloaded by the company. These failures resulted in hackers gaining access to personal information regarding 6.6 million consumers, over 500,000 of whom were U.S. consumers.

In addition to its enforcement efforts in the privacy and data security areas, the Commission seeks to improve agency decision-making through its policy initiatives. Last fall, for example, the Commission held four days of panels that specifically addressed consumer privacy and data security.[19] The Commission also announced its fourth PrivacyCon, which will take place on June 27, an annual event that explores evolving privacy and data security research.[20]

The Commission also is empowered to conduct industry studies related to privacy and data security under Section 6(b) of the FTC Act.[21] In March, we issued 6(b) orders to several internet service providers to evaluate their privacy practices.[22] As we have in the past, we will use the information we learn from this study to better inform our policy and enforcement work.

The Commission continues to work closely with our law enforcement partners in the European Union ("EU") and its member states to ensure the success of the EU-U.S. Privacy Shield framework. Under the EU's General Data Protection Regulation ("GDPR"), companies are required to meet certain data protection requirements in order to transfer consumer data from the EU to other jurisdictions. Privacy Shield—a voluntary mechanism that companies can use to comply with the

---

[19] *See* FTC Press Release, *FTC Announces Sessions on Consumer Privacy and Data Security as Part of Its Hearings on Competition and Consumer Protection in the 21st Century* (Oct. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its.
[20] *See* FTC Press Release, *FTC Announces PrivacyCon 2019 and Calls for Presentations* (Oct. 24, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/ftc-announces-privacycon-2019-calls-presentations.
[21] 15 U.S.C. § 46(b).
[22] *See* FTC Press Release, *FTC Seeks to Examine the Privacy Practices of Broadband Providers* (Mar. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-examine-privacy-practices-broadband-providers.

GDPR when transferring data from Europe to the United States and which facilitates billions of dollars in transatlantic data flows—is enforced by the FTC with respect to those participants under its jurisdiction.[23]

Last fall, for example, the Commission announced settlements with four companies that we alleged had falsely claimed Privacy Shield certification.[24] And in September 2018, Chairman Simons, along with the Secretary of Commerce and our European counterparts, participated in the second annual review of the Privacy Shield framework, culminating in a European Commission recommendation for continued FTC enforcement in the Privacy Shield area.[25] Our Privacy Shield approach is built on four pillars: referrals from the Department of Commerce; priority consideration of referrals from the European Union; checking for Privacy Shield violations as part of every privacy investigation; and proactive monitoring of Privacy Shield participants.

Finally, many of the FTC's privacy and data security investigations and cases involve complex facts and technologies and well-financed defendants, often requiring outside experts, which can be costly. It is critical that the FTC have sufficient resources to support its investigative and litigation needs, including expert work, particularly as demands for enforcement in this area continue to grow.

B. Protecting Consumers from Fraud

Fighting fraud is a major focus of the FTC's law enforcement efforts. The Commission's anti-fraud program tracks down and stops some of the most egregious scams that prey on U.S.

---

[23] *See* www.privacyshield.gov and www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield. Companies can also join a Swiss-U.S. Privacy Shield for transfers from Switzerland.

[24] *See* FTC Press Release, *FTC Reaches Settlements with Four Companies That Falsely Claimed Participation in the EU-U.S. Privacy Shield* (Sept. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/09/ftc-reaches-settlements-four-companies-falsely-claimed.

[25] *See Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield*, COM (2018) 860 final, https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf.

consumers—often, the most vulnerable consumers who can least afford to lose money. In 2018, imposter scams became the top consumer fraud complaint, in part due to the rise in reports about government imposter scams.[26] Fraudsters falsely claiming to be government agents (including the Social Security Administration, IRS and even the FTC), family members, or well-known tech companies contact consumers. These fraudsters pressure them to send money, often via cash-like payment methods, such as gift cards or money transfers, or trick them into providing personal information. Many of these scams target older Americans.

In response to the rise in imposter complaints, the FTC has filed multiple cases against defendants who deceptively pose as the government or well-known tech companies. For example, the FTC recently brought two actions against defendants for falsely claiming affiliations with the federal government. The Commission charged Sunkey Publishing with using copycat military recruitment websites to trick consumers seeking military careers into providing their personal information; according to the complaint, Sunkey then sold the information to post-secondary schools as part of its lead generation business.[27] The Commission's action against American Immigration Center stopped an alleged scheme using deceptive websites and advertising that falsely implied an affiliation with the U.S. Citizenship and Immigration Services to dupe legal residents trying to renew their green cards or apply for naturalization.[28]

---

[26] FTC Press Release, *Imposter Scams Top Complaints Made to FTC in 2018* (Feb. 28, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/imposter-scams-top-complaints-made-ftc-2018.
[27] FTC Press Release, FTC, *FTC Takes Action against the Operators of Copycat Military Websites* (Sept. 6, 2018), https://www.ftc.gov/news-events/press-releases/2018/09/ftc-takes-action-against-operators-copycat-military-websites.
[28] FTC Press Release, *American Immigration Center Settles with FTC on Government Imposter Allegations* (Oct. 16, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/american-immigration-center-settles-ftc-government-imposter. The court entered the Stipulated Order for Permanent Injunction and Monetary Judgment against the defendants on December 7, 2018.[29] FTC Press Release, *FTC Halts Tech Support Scam as Part of Major Initiative Focused on Older Adults Hit Hardest by These Scams* (Mar. 7, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-halts-tech-support-scam-part-major-initiative-focused-older.

The Commission also helps older Americans protect themselves from fraud. Last month, the FTC joined federal, state, and international law enforcement partners in announcing a nationwide and international crackdown on elder fraud schemes with a particular focus on technical support scams. Technical support scams dupe consumers into believing their computers are infected with viruses and malware, and then charge them hundreds of dollars for unnecessary repairs. As part of that initiative, the FTC filed suit against technical support operator Elite IT Partners,[29] developed new consumer education materials to help consumers avoid falling victim to these scams,[30] and released new complaint data that illustrates the disproportionate effect these scams have on older adults.[31]

Over the last year, the FTC has targeted business opportunity scams, filing numerous actions against defendants who promise consumers a legitimate opportunity to earn money if consumers will pay for defendants' "coaching" services. In reality, the "coaching" services provide no value to consumers and are typically nothing more than a handful of training videos and documents with generic information. In Digital Altitude, the Commission brought an action against defendants who allegedly defrauded consumers out of millions of dollars—some paying more than $50,000—by promising of individualized coaching on how to run an online business.[32] The Commission also brought separate actions against defendants in FBA Stores[33] and, with the

---

[29] FTC Press Release, *FTC Halts Tech Support Scam as Part of Major Initiative Focused on Older Adults Hit Hardest by These Scams* (Mar. 7, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-halts-tech-support-scam-part-major-initiative-focused-older.
[30] *See* How to Spot, Avoid and Report Tech Support Scams, https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams.
[31] *See* FTC Consumer Protection Data Spotlight, *Older Adults Hardest Hit by Tech Support Scams* (Mar. 7, 2019), https://www.ftc.gov/news-events/blogs/data-spotlight/2019/03/older-adults-hardest-hit-tech-support-scams.
[32] FTC Press Release, *FTC Obtains Court Order Halting Business Coaching Scheme* (Feb. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/ftc-obtains-court-order-halting-business-coaching-scheme.
[33] FTC Press Release, *FTC Action Halts a Large Deceptive Business Opportunity Scheme* (Mar. 23, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/ftc-action-halts-large-deceptive-business-opportunity-scheme.

Attorney General of Minnesota, against defendants in Sellers Playbook[34] based on allegations that the defendants falsely claimed they could teach consumers "the secrets for making money on Amazon." The Commission's actions shut down three large operations that resulted in over $100 million in losses to consumers.

The Commission's fraud cases also extend to sprawling international scams. The Commission charged the defendants in MOBE—competitors of Digital Altitude—for running an international coaching scam that the FTC alleged took more than $300 million from thousands of American consumers.[35] The Commission also recently filed an action against defendants in Sanctuary Belize, a massive land sale scam that allegedly bilked over $100 million from consumers, largely retirees. According to the complaint, recidivist Andris Pukke perpetrated an international scheme selling lots in a development in remote southern Belize with promises that he never intended to keep. The FTC shut down the enterprise by obtaining a temporary restraining order and preliminary injunction, and continues to litigate the matter.[36]

The FTC frequently works with other law enforcement agencies to tackle widespread fraud. In July 2018, the FTC launched "Operation Donate with Honor," a coordinated effort to target fraudulent and deceptive fundraising for military and veterans' causes that has resulted in over 100 law enforcement actions.[37] As part of that initiative, the FTC has announced four cases with several

---

[34] FTC Press Release, *FTC and State of Minnesota Halt Sellers Playbook's Get Rich Scheme* (Aug. 6, 2018), https://www.ftc.gov/news-events/press-releases/2018/08/ftc-state-minnesota-halt-sellers-playbooks-get-rich-scheme.
[35] FTC Press Release, *FTC Action Halts MOBE, a Massive Internet Business Coaching Scheme* (June 11, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftc-action-halts-mobe-massive-internet-business-coaching-scheme.
[36] FTC Press Release, *At FTC's Request, Court Halts Massive "Sanctuary Belize" Real Estate Investment Scam* (Nov. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/11/ftcs-request-court-halts-massive-sanctuary-belize-real-estate.
[37] FTC Press Release, *Operation Donate with Honor: Law Enforcers Unite to Challenge Deceptive Fundraising* (Jul. 19, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/07/operation-donate-honor-law-enforcers-unite-challenge. This initiative included 54 Attorneys General from all 50 states, the District of Columbia, American Samoa, Guam, and Puerto Rico, and 16 state agencies that oversee charities.

state Attorneys General to shut down sham charity operations that were using consumers' generous donations for private benefits and spent very little of the donated funds on the charitable programs.[38]

The FTC strives to stay ahead of scammers by analyzing Sentinel complaints to help raise public awareness about fraud. In October 2018, the FTC launched its *Consumer Protection Data Spotlight* series to alert law enforcers, industry, and the public about growing threats and important patterns identified in Sentinel data. The *Spotlight* explores data over time, showing how scammers change tactics and catch consumers off guard.[39] In addition, the FTC is making Sentinel data more accessible to state and local governments, the media, academics, and the public-at-large by publishing interactive dashboards that enable people to see what kind of fraud is affecting their state or large metropolitan area.[40]

C. Truthfulness in National Advertising

Ensuring that advertising is truthful and not misleading has long been one of the FTC's core missions. It allows consumers to make well-informed decisions about how to best use their resources and promotes the efficient functioning of market forces by encouraging the dissemination of accurate information.

---

[38] *FTC & State of Missouri v. Disabled Police and Sheriffs Foundation, Inc., et al.*, No. 4:19-cv-00667 (E.D. Mo. Mar. 28, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3128/disabled-police-sheriffs-foundation-inc; *FTC & State of Florida Office of the Attorney General v. American Veterans Foundation, Inc., et al.*, No. 8:18-cv-00744 (M.D. Fla. Mar. 28, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3163/american-veterans-foundation-inc; *FTC et al. v. Help the Vets, Inc., et al.*, No. 6:18-cv-1153-Orl-41KRS (M.D. Fla. July 19, 2018), https://www.ftc.gov/enforcement/cases-proceedings/172-3159/help-vets-inc; *FTC v. Travis Deloy Peterson*, No. 4:18-00049-DN (D. Utah July 16, 2018), https://www.ftc.gov/enforcement/cases-proceedings/182-3049/veterans-america.

[39] The first *Spotlight* identified a sharp rise in gift cards—particularly iTunes and Google Play cards—as a payment method for scams. *See* FTC Consumer Protection Data Spotlight, *Scammers Increasingly Demand Payment by Gift Card* (Oct. 2018), https://www.ftc.gov/news-events/blogs/data-spotlight/2018/10/scammers-increasingly-demand-payment-gift-card. Most recently, the Spotlight pointed to the dramatic increase in reports about imposters passing themselves off as Social Security Administration officials, which is happening just as reports about IRS imposter scams are waning. *See* FTC Consumer Protection Data Spotlight, *Growing Wave of Social Security Imposters Overtakes IRS Scam* (Apr. 2019), https://www.ftc.gov/news-events/blogs/data-spotlight/2019/04/growing-wave-social-security-imposters-overtakes-irs-scam.

[40] *See generally* FTC, *FTC Consumer Sentinel Network* (Apr. 8, 2019), https://public.tableau.com/profile/federal.trade.commission.

For example, the agency has continued to bring cases challenging false and unsubstantiated health claims, including those targeting older consumers, consumers affected by the opioid crisis, and consumers with serious medical conditions. The Commission has brought cases challenging products that claim to improve memory and ward off cognitive decline, relieve joint pain and arthritis symptoms, and even reverse aging.[41] We have challenged bogus claims that treatments could cure, treat, or mitigate various serious diseases and ailments, including those affecting children and older consumers.[42] We have brought law enforcement actions against advertisers and ad agencies who allegedly used native advertising—commercial advertising masquerading as editorial content—to deceptively sell health products such as mosquito repellants during the Zika virus outbreak and cognitive improvement supplements.[43] The Commission also has sued companies that claimed, allegedly without scientific evidence, that using their products could alleviate the symptoms of opioid withdrawal and increase the likelihood of overcoming opioid dependency.[44] The Commission obtained an order barring a marketer from making deceptive claims about its products' ability to mitigate the side effects of cancer treatments.[45] And we have issued

---

[41] *See, e.g.*, *Telomerase Activation Sci., Inc. et al.*, No. C-4644 (Apr. 19, 2018), https://www.ftc.gov/enforcement/cases-proceedings/142-3103/telomerase-activation-sciences-inc-noel-thomas-patton-matter; *FTC v. Health Research Labs., Inc.*, No. 2:17-cv-00467 (D. Maine Nov. 30, 2017), https://www.ftc.gov/enforcement/cases-proceedings/152-3021/health-research-laboratories-llc.

[42] *See, e.g.*, *FTC v. Regenerative Med. Grp., Inc.*, No. 8:18-cv-01838 (C.D. Cal. filed Oct. 12, 2018), https://www.ftc.gov/enforcement/cases-proceedings/172-3062/regenerative-medical-group-inc; *A&O Enters., Inc.*, No. C-4670 (Feb. 21, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3016/ao-enterprises-doing-business-iv-bars-aaron-k-roberts-matter.

[43] *See, e.g.*, *FTC v. Glob. Cmty. Innovations LLC*, No. 5:19-CV-00788 (N.D. Ohio Apr. 10, 2019), https://www.ftc.gov/enforcement/cases-proceedings/162-3135/global-community-innovations-llc-et-al-geniux; *Creaxion Corp.*, No. C-4668 (Feb. 8, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3066/creaxion-corp; *Inside Publ'ns, LLC*, No. C-4669 (Feb. 8, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3067/inside-publications-llc.

[44] *FTC v. Catlin Enters., Inc.*, No. 1:17-cv-403 (W.D. Tex. May 17, 2017), https://www.ftc.gov/enforcement/cases-proceedings/1623204/catlin-enterprises-inc. In addition, in conjunction with the FDA, the FTC issued letters to companies that appeared to be making questionable claims in order to sell addiction or withdrawal remedies. *See* FTC Press Release, *FTC, FDA Warn Companies about Marketing and Selling Opioid Cessation Products* (Jan. 24, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/ftc-fda-warn-companies-about-marketing-selling-opioid-cessation.

[45] *FTC v. CellMark Biopharm*, No. 2:18-cv-00014-JES-CM (M.D. Fla. Jan. 12, 2018), https://www.ftc.gov/enforcement/cases-proceedings/162-3134/cellmark-biopharma-derek-e-vest.

joint warning letters with the Food and Drug Administration to marketers who claim their dietary supplements and cannabidiol ("CBD") products treat or prevent serious diseases, including Alzheimer's disease and cancer.[46]

When consumers with serious health concerns fall victim to unsupported health claims, they may put their health at risk by avoiding proven therapies and treatments. Through consumer education, including the FTC's advisories, the agency urges consumers to check with a medical professional before starting any treatment or product to treat serious medical conditions.[47]

D. Illegal Robocalls

Illegal robocalls also remain a significant consumer protection problem and one of consumers' top complaints to the FTC. These calls disturb consumers' privacy, and frequently use fraud and deception to pitch goods and services, leading to significant economic harm. In FY 2018, the FTC received more than 5.7 million complaints about unwanted calls, including 3.7 million complaints about robocalls.[48] The FTC has used all the tools at its disposal to fight these illegal calls, including 141 enforcement actions to date.[49]

---

[46] *See* FTC Press Release, *FTC Joins FDA in Sending Warning Letters to Companies Advertising and Selling Products Containing Cannabidiol (CBD) Claiming to Treat Alzheimer's, Cancer, and Other Diseases* (Apr. 2, 2019), https://www.ftc.gov/news-events/press-releases/2019/04/ftc-joins-fda-sending-warning-letters-companies-advertising; FTC Press Release, *FTC and FDA Send Warning Letters to Companies Selling Dietary Supplements Claiming to Treat Alzheimer's Disease and Remediate or Cure Other Serious Illnesses Such as Parkinson's, Heart Disease, and Cancer* (Feb. 11, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/ftc-fda-send-warning-letters-companies-selling-dietary.

[47] FTC Consumer Blog, *Treatments and Cures*, https://www.consumer.ftc.gov/topics/treatments-cures.

[48] *See Do Not Call Registry Data Book 2018: Complaint Figures for FY 2018*, https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2018.

[49] *See* FTC Robocall Initiatives, https://www.consumer.ftc.gov/features/feature-0025-robocalls. Since establishing the Do Not Call Registry in 2003, the Commission has fought vigorously to protect consumers' privacy from unwanted calls. Indeed, since the Commission began enforcing the Do Not Call provisions of the Telemarketing Sales Rule ("TSR") in 2004, the Commission has brought enforcement actions seeking civil penalties, restitution for victims of telemarketing scams, and disgorgement of ill-gotten gains against 444 corporations and 358 individuals. As a result of the 125 cases resolved thus far, the Commission has collected over $121 million in equitable monetary relief and civil penalties. *See* Enforcement of the Do Not Call Registry, https://www.ftc.gov/news-events/media-resources/do-not-call-registry/enforcement. In August 2017, the FTC and its law enforcement partners achieved an historic win in a long-running fight against unwanted calls when a federal district court in Illinois issued an order imposing a $280 million

The FTC's most recent law enforcement crackdown stopped four separate robocall operations.[50] For example, in *FTC v. Christiano*, the FTC obtained a $1.35 million civil penalty and a ban on providing an autodialer to anyone engaged in telemarketing against two technology companies and their owner for knowingly providing the tools that unlawful telemarketers used to blast out billions of illegal robocalls.[51] In another case from the recent crackdown,[52] the FTC sued a recidivist robocaller and his partners for allegedly running a Google rankings scam that used robocalls to reach their victims and bombarded individuals who did not own businesses with the same robocalls.[53] In April, a court granted the FTC's motion for summary judgment, banning him and one of his co-defendants from all telemarketing and imposing a $3.3 million judgment.

Despite the FTC's vigorous law enforcement program, technological advances continue to permit bad actors to place millions or even billions of calls, often from abroad, at very low cost, and in ways that are difficult to trace. This phenomenon continues to infuriate consumers and challenge enforcers. Recognizing that law enforcement, while critical, is not enough to solve the problem of illegal calls, the FTC has taken steps to spur the marketplace to develop technological solutions. For instance, from 2013 to 2015, the FTC led four public challenges to incentivize innovators to help tackle the unlawful robocalls that plague consumers.[54] The FTC's challenges contributed to a shift

---

penalty against Dish Network—the largest penalty ever issued in a Do Not Call case. *U.S. et al. v. Dish Network, L.L.C.*, No. 309-cv-03073-JES-CHE (C.D. Ill. Aug. 10, 2017), https://www.ftc.gov/enforcement/cases-proceedings/052-3167/dish-network-llc-united-states-america-federal-trade.

[50] *See* FTC Press Release, *FTC Crackdown Stops Operations Responsible for Billions of Illegal Robocalls* (Mar. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-crackdown-stops-operations-responsible-billions-illegal.

[51] *FTC v. James Christiano et al.*, No. 8:18-cv-00936 (C.D. Cal. June 5, 2018), https://www.ftc.gov/enforcement/cases-proceedings/162-3124/james-christiano-et-al-netdotsolutions-inc.

[52] *FTC v. Pointbreak Media LLC et al.*, No. 18-cv-61017 (S.D. Fla. May 23, 2018), https://www.ftc.gov/enforcement/cases-proceedings/172-3182/pointbreak-media-llc-0.

[53] Previously, in 2017, the FTC settled claims with Ramsey for illegal robocalls and calls to numbers listed on the National Do Not Call Registry. *See FTC v. Ramsey et al.*, No. 9:17-cv-80032 (S.D. Fla. Jan. 13, 2017), https://www.ftc.gov/enforcement/cases-proceedings/132-3254/justin-ramsey.

[54] The first challenge, in 2013, called upon the public to develop a consumer-facing solution to block illegal robocalls. One of the winners, "NomoRobo," was on the market within 6 months after being selected by the FTC. NomoRobo, which reports blocking over 600 million calls to date, is being offered directly to consumers by a number of

in the development and availability of technological solutions in this area, particularly call-blocking and call-filtering products. Consumers can access information about potential solutions available to them on the FTC's website.[55] The telecommunications industry has also developed a new framework, SHAKEN/STIR, which is designed to limit illegitimate number spoofing and reduce illegal robocalls.

The FTC continues to engage with industry stakeholders and supports the industry initiative to authenticate caller ID numbers. The FTC also regularly works with its state, federal, and international partners to combat illegal robocalls.[56]

For many years, the Commission has recommended eliminating the common carrier exemption. The exemption is outdated and no longer makes sense in today's marketplace where the lines between telecommunications and other services are increasingly blurred. It impedes the FTC's work tackling illegal robocalls and more broadly circumscribes other enforcement initiatives. For example, a carrier that places, or assists and facilitates, illegal telemarketing might argue that it is beyond the Commission's reach because of the common carrier exemption. Likewise, the exemption may frustrate the Commission's ability to obtain complete relief for consumers when

---

telecommunications providers and is available as an app on iPhones. *See* Press Release, *FTC Announces Robocall Challenge Winners* (Apr. 2, 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-announces-robocall-challenge-winners; *see also* Press Release, *FTC Awards $25,000 Top Cash Prize for Contest-Winning Mobile App That Blocks Illegal Robocalls* (Aug. 17, 2015), https://www.ftc.gov/news-events/press-releases/2015/08/ftc-awards-25000-top-cash-prize-contest-winning-mobile-app-blocks; Press Release, *FTC Announces Winners of "Zapping Rachel" Robocall Contest* (Aug. 28, 2014), https://www.ftc.gov/news-events/press-releases/2014/08/ftc-announces-winners-zapping-rachel-robocall-contest.

[55] *See* https://www.consumer.ftc.gov/features/how-stop-unwanted-calls.

[56] *See, e.g.*, FTC Press Release, *FTC and FCC to Host Joint Policy Forum on Illegal Robocalls* (Mar. 22, 2018), www.ftc.gov/news-events/press-releases/2018/03/ftc-fcc-host-joint-policy-forum-illegal-robocalls; FTC Press Release, *FTC and FCC Seek Exhibitors for an Expo Featuring Technologies to Block Illegal Robocalls* (Mar. 7, 2018), www.ftc.gov/news-events/press-releases/2018/03/ftc-fcc-seek-exhibitors-expo-featuring-technologies-block-illegal; Memorandum of Understanding Among Public Authorities of the Unsolicited Communications Enforcement Network Pertaining to Unlawful Telecommunications and SPAM (May 2016), https://www.ftc.gov/policy/cooperation-agreements/international-unlawful-telecommunications-spam-enforcement-cooperation; FTC Press Release, *FTC Signs Memorandum of Understanding With Canadian Agency To Strengthen Cooperation on Do Not Call, Spam Enforcement* (Mar. 24, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-signs-memorandum-understanding-canadian-agency-strengthen.

there are multiple parties, some of whom are common carriers. It also may pose difficulties when a company engages in deceptive or unfair practices involving a mix of common carrier and non-common carrier activities. Finally, litigation has been complicated by entities that attempt to use their purported status as common carriers to shield themselves from FTC enforcement.[57]

E. Consumer and Business Education and Outreach

Public outreach and education is another critical element of the FTC's efforts to fulfill its consumer protection mission. The Commission's education and outreach programs reach tens of millions of people each year through the FTC's website, the media, and partner organizations that disseminate consumer information on the agency's behalf. The FTC delivers actionable, practical, plain-language guidance on dozens of issues, and updates its consumer education materials whenever it has new information to share.

The FTC disseminates these tips through articles, blog posts, infographics, videos, social media, and education campaigns. For example, in response to the enactment of the Economic Growth, Regulatory Relief, and Consumer Protection Act,[58] which allows consumers nationwide to freeze their credit and place year-long fraud alerts for free, the Commission helped consumers take advantage of the new protections by: updating IdentityTheft.gov; revising its identity theft publications; and providing blogs, webinars, and podcasts in collaboration with a wide range of partners.[59]

---

[57] *See, e.g.*, Answer and Affirmative Defenses of Defendant Pacific Telecom Communications Group at 9, 17-20, Dkt. 19, *FTC et al. v. Caribbean Cruise Line et al.*, No. 0:15-cv-60423 (S.D. Fla. June 2, 2015), https://www.ftc.gov/enforcement/cases-proceedings/122-3196-x150028/caribbean-cruise-line-inc.
[58] Pub. L. No: 115-174.
[59] *See* FTC Press Release, *Starting Today, New Federal Law Allows Consumers to Place Free Credit Freezes and Yearlong Fraud Alerts* (Sept. 21, 2018), https://www.ftc.gov/news-events/press-releases/2018/09/starting-today-new-law-allows-consumers-place-free-credit-freezes.

The FTC also tailors its guidance to serve specific audiences, including older adults.[60] A recent FTC report to Congress details how older adults experience scams,[61] and a series of FTC *Data Spotlights* gives further details on scams that affect older adults[62] and helps educate consumers.[63]

The Commission also works to provide companies with resources on a variety of issues that affect businesses. For example, our "Cybersecurity for Small Business" campaign, a joint effort with the National Institute of Standards and Technology, the Small Business Administration, and the Department of Homeland Security, includes a dozen need-to-know topics as well as fact sheets, videos, and other materials.[64]

IV. COMPETITION MISSION

In addition to the consumer protection work described above, the FTC enforces U.S. antitrust law in many sectors that directly affect consumers and their wallets, such as health care, consumer products and services, technology, manufacturing, and energy. The Commission shares federal antitrust enforcement responsibilities with the Antitrust Division of the U.S. Department of Justice ("DOJ").

One of the agencies' principal responsibilities is to prevent mergers that may substantially lessen competition. Under U.S. law, parties to certain mergers and acquisitions must file premerger notification with the FTC and DOJ and observe the statutorily prescribed waiting period before

---

[60] *See* www.ftc.gov/PassItOn and www.ftc.gov/Pasalo. The campaign has distributed more than 10.6 million print publications since its creation, including 1.1 million so far in fiscal year 2019.
[61] FTC Report, *Protecting Older Consumers: 2017-2018* (Oct. 2018), https://www.ftc.gov/reports/protecting-older-consumers-2017-2018-report-congress-federal-trade-commission.
[62] *See, e.g.*, FTC Consumer Protection Data Spotlight, *Older Adults Hardest Hit by Tech Support Scams* (Mar. 7, 2019), https://www.ftc.gov/news-events/blogs/data-spotlight/2019/03/older-adults-hardest-hit-tech-support-scams.
[63] *See, e.g.*, FTC Consumer Blog, *How to Spot, Avoid, and Report Tech Support Scams* (Feb. 2019), https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams and https://www.consumidor.ftc.gov/articulos/como-detectar-evitar-y-reportar-las-estafas-de-soporte-tecnico.
[64] *See Cybersecurity Resources for Your Small Business* (Oct. 18, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/10/cybersecurity-resources-your-small-business. These materials will soon be available in Spanish.

consummating their transactions. Premerger filings under the Hart-Scott-Rodino ("HSR") Act have generally increased steadily since FY 2013. Last year, for the second year in a row, we received just over 2,000 HSR filings.[65]

Most reported transactions do not raise significant competitive concerns and the agencies clear those non-problematic transactions expeditiously. But when the evidence suggests that a proposed merger likely would be anticompetitive, the Commission does not hesitate to intervene. In FY 2018, the Commission took enforcement actions against 22 different mergers, most of which were resolved through a consent decree. We also challenged five mergers in court: federal courts granted preliminary injunctions in two cases;[66] the parties abandoned their plans in the face of our court challenge in two cases;[67] and a ruling is currently pending in the fifth matter.[68]

One increasing challenge for the Commission in litigating competition cases is the continuing need to hire testifying economic experts. Qualified experts are critically important in competition cases heading to litigation. Although the agency thus far has managed to find sufficient resources to fund the experts needed to support its cases, the FTC appreciates Congress's attention to its resource needs, including the need to hire outside experts.

Over the past year, the Commission has continued its decades-long efforts to fight anti-competitive conduct in the pharmaceuticals and health care industries, where rising costs continue

[65] The agencies received 2,111 HSR filings in FY 2018, a slight increase from FY 2017, where we received 2,052. Apart from the last two years, the last time annual HSR notification filings exceeded 2,000 was back in FY 2007. For historical information about HSR filings and U.S. merger enforcement, see the joint FTC/DOJ Hart-Scott-Rodino annual reports, https://www.ftc.gov/policy/reports/policy-reports/annual-competition-reports.

[66] *See, FTC v. Tronox Ltd.*, 332 F. Supp. 3d 187 (D.D.C. 2018), (granting preliminary injunction); *FTC v. Wilh. Wilhelmsen Holding ASA*, 341 F. Supp. 3d 27 (D.D.C. 2018) (granting preliminary injunction). The agency also won a full administrative trial on the merits in the *Tronox* matter before an administrative law judge, before the parties ultimately settled with the agency. FTC Press Release, *FTC Requires Divestitures by Tronox and Cristal, Suppliers of Widely Used White Pigment, Settling Litigation over Proposed Merger* (Apr. 10, 2019), https://www.ftc.gov/news-events/press-releases/2019/04/ftc-requires-divestitures-tronox-cristal-suppliers-widely-used.

[67] J.M. Smuckers and Conagra abandoned their planned combination after the FTC filed suit in March 2018. CDK abandoned its plan to purchase Auto-Mate after the Commission initiated litigation in March 2018.

[68] The agency formally challenged the consummated merger of Otto Bock and Freedom Innovations in FY 2018. Litigation before an administrative law judge concluded last fall and the agency is currently awaiting a ruling.

to burden American consumers. For over twenty years, the Commission has prioritized ending anticompetitive reverse payment agreements in which a brand-name drug firm pays its potential generic rival to delay entering the market with a lower cost generic product. Following the U.S. Supreme Court's 2013 decision in *FTC v. Actavis, Inc.*,[69] the Commission is in a much stronger position to protect consumers. Since that ruling, the FTC obtained a landmark $1.2 billion settlement in its litigation involving the sleep disorder drug, Provigil,[70] and other manufacturers, including the remaining *Actavis* defendants,[71] have agreed to abandon the practice.[72] In administrative litigation, the Commission ruled in March of this year that Impax had engaged in an illegal reverse payment agreement designed to block consumers' access to a lower-cost generic version of the branded drug, Opana ER.[73] In addition, the Commission has challenged other anticompetitive conduct by drug manufacturers. Last month, the Commission filed a complaint against the health information company Surescripts, alleging that it employed illegal vertical and horizontal restraints to maintain its monopolies over two electronic prescribing, or "e-prescribing," markets (routing and eligibility).[74] Additionally, a federal court recently ruled that AbbVie Inc. used sham litigation illegally to maintain its monopoly over the testosterone replacement drug

[69] 570 U.S. 756 (2013). On February 28, 2019, after over ten years of litigation, the Commission reached a settlement with the final remaining defendant in the *Actavis* case.
[70] FTC Press Release, *FTC Settlement of Cephalon Pay for Delay Case Ensures $1.2 Billion in Ill-Gotten Gains Relinquished; Refunds Will Go To Purchasers Affected by Anticompetitive Tactics* (May 28, 2015), https://www.ftc.gov/news-events/press-releases/2015/05/ftc-settlement-cephalon-pay-delay-case-ensures-12-billion-ill.
[71] FTC Press Release, *Last Remaining Defendant Settles FTC Suit that Led to Landmark Supreme Court Ruling on Drug Company "Reverse Payments"* (Feb. 28, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/last-remaining-defendant-settles-ftc-suit-led-landmark-supreme.
[72] FTC Press Release, *FTC Enters Global Settlement to Resolve Reverse-Payment Charges against Teva* (Feb. 9, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/ftc-enters-global-settlement-resolve-reverse-payment-charges; Joint Motion for Entry of Stipulated Order for Permanent Injunction, *FTC v. Allergan plc*, No. 17-cv-00312 (N.D. Cal. Jan. 23, 2017), https://www.ftc.gov/enforcement/cases-proceedings/141-0004/allergan-plc-watson-laboratories-inc-et-al; Stipulated Order for Permanent Injunction, *FTC v. Teikoku Pharma USA, Inc.*, No. 16-cv-01440 (E.D. Pa. Mar. 30, 2016), https://www.ftc.gov/enforcement/cases-proceedings/141-0004/endo-pharmaceuticals-impax-labs.
[73] FTC Press Release, *FTC Concludes that Impax Entered into Illegal Pay-for-Delay Agreement* (Mar. 29, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-concludes-impax-entered-illegal-pay-delay-agreement.
[74] FTC Press Release, *FTC Charges Surescripts with Illegal Monopolization of E-Prescription Markets* (Apr. 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/04/ftc-charges-surescripts-illegal-monopolization-e-prescription.

Androgel, and ordered $493.7 million in monetary relief to consumers who were overcharged for Androgel as a result of AbbVie's conduct.[75]

The Commission also maintains a robust program to identify and stop anticompetitive conduct. This year, in administrative litigation of the *1-800 Contacts* matter, the Commission ruled that agreements among competitors to limit the scope of their internet advertising were unlawful.[76] The agency also successfully argued and won an important procedural victory in the U.S. Court of Appeals for the Fifth Circuit, defeating an effort by the Louisiana Real Estate Appraisers Board to obtain interlocutory review of the agency's determination that the state-action doctrine did not apply to its conduct.[77] The agency also has several other conduct matters in active litigation.[78]

The Commission also continues to focus its attention on high technology markets. In an effort to more closely monitor developments in the technology sector, the FTC's Bureau of Competition recently announced the creation of a Technology Task Force dedicated to monitoring competition in U.S. technology markets.[79] The Task Force will include attorneys from the Bureau of Competition with expertise in complex product and service markets and ecosystems, including markets for online advertising, social networking, mobile operating systems and apps, and platforms, and will be supported by a Technology Fellow who will provide important technical assistance for investigations. The Task Force will examine industry practices, conduct law

---

[75] *FTC v. AbbVie Inc.*, 329 F. Supp. 3d 98 (E.D. Pa. 2018); Statement of FTC Chairman Joe Simons Regarding Federal Court Ruling in *FTC v. AbbVie* (June 29, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/statement-ftc-chairman-joe-simons-regarding-federal-court-ruling.

[76] *In re 1-800 Contacts, Inc.*, Dkt. No. 9372 (Nov. 14, 2018), https://www.ftc.gov/system/files/documents/cases/docket_no_9372_opinion_of_the_commission_redacted_public_version.pdf. This matter is currently on appeal to the U.S. Court of Appeals for the Second Circuit.

[77] *La. Real Estate Appraisers Bd. v. FTC*, 917 F.3d 389 (5th Cir. 2019).

[78] In addition to the cases involving pharmaceutical firms discussed *infra*, pending litigation alleging anticompetitive conduct includes *FTC v. Qualcomm, Inc.*, No. 17-cv-00220 (N.D. Cal. Jan. 17, 2017), https://www.ftc.gov/enforcement/cases-proceedings/141-0199/qualcomm-inc; *In re Benco Dental Supply et al.*, Dkt. No. 9379 (Feb. 12, 2018), https://www.ftc.gov/enforcement/cases-proceedings/151-0190/bencoscheinpatterson-matter.

[79] FTC Press Release, *FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets* (Feb. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology.

enforcement investigations, and coordinate and consult with staff throughout the FTC on technology-related matters, including prospective merger reviews and reviews of consummated technology mergers.

In addition to competition enforcement, the FTC promotes competition principles in advocacy comments to state lawmakers and regulators, as well as to its sister federal agencies[80] and in amicus briefs filed in federal courts considering important areas of antitrust law.[81] The Commission benefits from critical self-examination, examining prior merger enforcement decisions to assess their impact on competition and consumers, and we intend to expand this effort going forward. Similarly, through the series of hearings described above, the Commission is devoting significant resources to refresh and, if warranted, renew its thinking on a wide range of cutting-edge competition issues.[82]

V. INTERNATIONAL COOPERATION

The FTC also engages in significant international work to support its domestic enforcement programs. During the last fiscal year, the FTC cooperated in 43 investigations, cases, and enforcement projects with foreign consumer, privacy, and criminal enforcement agencies. To sustain this level of cooperation, the agency often works through global enforcement networks, such as the International Consumer Protection and Enforcement Network, the Global Privacy Enforcement Network, the Unsolicited Communications Enforcement Network, and the International Mass Marketing Fraud Working Group. The FTC also works directly with foreign counterparts on enforcement issues.[83]

---

[80] *See generally* https://www.ftc.gov/policy/advocacy.
[81] Amicus briefs are posted at https://www.ftc.gov/policy/advocacy/amicus-briefs.
[82] *See* Prepared Remarks of Chairman Simons Announcing the Competition and Consumer Protection Hearings (June 20, 2018), https://www.ftc.gov/system/files/documents/public_statements/1385308/prepared_remarks_of_joe_simons_announcing_the_hearings_6-20-18_0.pdf.
[83] For example, the FTC has conducted several trainings and roundtables in the United States and India to help develop

International enforcement cooperation also is critical for the FTC's competition program. With the expansion of global trade and the operation of many companies across national borders, the FTC and DOJ increasingly engage with foreign antitrust agencies to ensure close collaboration on cross-border cases and convergence toward sound competition policies and procedures.[84] The FTC effectively coordinates reviews of multijurisdictional mergers and continues to work with its international counterparts to achieve consistent outcomes in cases of possible anticompetitive conduct. The U.S. antitrust agencies facilitate dialogue and promote convergence through multiple channels, including through strong bilateral relations with foreign competition agencies and multilateral competition organization projects and initiatives. The FTC also works with other agencies within the U.S. government to advance consistent competition enforcement policies, practices, and procedures in other parts of the world.[85]

The U.S. SAFE WEB Act is key to much of the agency's international work, especially on consumer protection and privacy matters.[86] Passed in 2006 and renewed in 2012, the Act strengthens the FTC's ability to work on cases with an international dimension. It allows the FTC to share evidence and provide investigative assistance to foreign authorities in cases involving spam, spyware, misleading health and safety claims, privacy violations and data security breaches, and telemarketing fraud. In many cases, the foreign agencies investigated conduct that directly

---

the capacity of Indian law enforcement to address tech support and other impostor scams such as the impersonation of IRS and Social Security officials. To address these continued threats, the FTC will convene a fourth annual roundtable in June, in partnership with the U.S.-India Business Council, on combatting Indian call center fraud. U.S.-India Business Council, *4th Annual Round Table on Stepping Up to Stop Indian Call Center Fraud*, https://www.usibc.com/event/4th-annual-round-table-on-stepping-up-to-stop-indian-call-center-fraud.

[84] In competition matters, the FTC also seeks to collaborate with the state Attorneys General to maximize results and use of limited resources in the enforcement of the U.S. antitrust laws.

[85] For example, the Commission works through the U.S. government's interagency processes to ensure that competition-related issues that also implicate broader U.S. policy interests, such as the protection of intellectual property and non-discrimination, are addressed in a coordinated and effective manner.

[86] Undertaking Spam, Spyware, and Fraud Enforcement With Enforcers Beyond Borders Act (U.S. SAFE WEB Act), Pub. L. No. 109-455, 120 Stat. 3372, extended by Pub. L. No. 112-203, 126 Stat. 1484 (amending 15 U.S.C. §§ 41 et seq.). Certain provisions, such as the secondment program for foreign officials described below, also apply to the FTC's competition work.

harmed U.S. consumers; in others, the FTC's action led to reciprocal assistance. The Act also has bolstered the agency's authority to engage in enhanced enforcement cooperation with foreign counterparts, including through memoranda of understanding, international agreements, staff exchanges, and other mechanisms.

The U.S. SAFE WEB Act has been a remarkable success. The Act enabled the FTC to respond to more than 130 SAFE WEB information sharing requests from more than 30 foreign enforcement agencies. It allowed the FTC to issue more than 115 civil investigative demands in more than 50 investigations on behalf of foreign agencies, both civil and criminal. The Commission has also used this authority to file suit in federal court to obtain judicial assistance for one of its closest law enforcement partners, the Canadian Competition Bureau.[87]

The FTC's foreign law enforcement partners similarly have assisted FTC enforcement actions. For example, the FTC worked directly with U.K. and Canadian authorities to halt Next-Gen Inc., a sweepstakes scam.[88] The FTC relied on key information sharing provisions of the U.S. SAFE WEB Act to facilitate cooperation with its U.K. partner and, last month, the defendants forfeited $30 million in cash and assets to settle the FTC's charges. In the privacy arena, the FTC used key provisions of the U.S. SAFE WEB Act to collaborate successfully with the Office of the Privacy Commissioner of Canada in its COPPA case against V-Tech, the FTC's first case involving Internet-connected toys.[89] The FTC also brought several significant enforcement actions in the past year relying on the SAFE WEB Act's provisions that allow the FTC to reach foreign conduct that has a "reasonably foreseeable" effect on U.S. consumers, or that involves "material conduct" in the

[87] *See* Remarks by John Pecman, Commissioner of Competition [Canada] at International Privacy Enforcement Meeting (June 4, 2015), https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03957.html.
[88] FTC Press Release, *Operators of Sweepstakes Scam Will Forfeit $30 Million to Settle FTC Charges* (Mar. 7, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/operators-sweepstakes-scam-will-forfeit-30-million-settle-ftc.
[89] *U.S. v. VTech Electronics Ltd., et al.*, No. 1:18-cv-00114 (N.D. Ill. Jan. 8, 2018), https://www.ftc.gov/enforcement/cases-proceedings/162-3032/vtech-electronics-limited.

United States, as the basis for challenging practices involving foreign defendants.[90]

The Act also underpins the FTC's ability to participate in cross-border cooperation arrangements. This includes data transfer mechanisms such as the EU-U.S. Privacy Shield framework and the Swiss-U.S. Privacy Shield framework, as well as the APEC Cross-Border Privacy Rules System, designed to protect privacy and data flows in the Asia-Pacific region. Many U.S. companies use these mechanisms to carry out cross-border data flows consistent with strong privacy protections. The SAFE WEB Act also provides the FTC with key powers helping to carry out enhanced cooperation with important partners.[91]

The SAFE WEB Act's provision authorizing staff exchanges also yields tremendous benefits. Using the Act, the FTC established an International Fellows program that has enabled the agency to host over 120 officials of foreign competition, consumer protection, and data privacy agencies to work alongside FTC staff on enforcement matters, subject to confidentiality protections, over the past dozen years. Foreign counterparts continue to seek exchanges with us, as the Fellows incorporate their learning from the FTC into the work of their home agencies, strengthening their capacity as well as our cooperative relationships with those counterparts.

The Act sunsets in 2020. The Commission strongly urges Congress to reauthorize this critical authority and eliminate the sunset provision. Just as Congress permanently granted the

---

[90] *See, e.g.*, FTC Press Release, *Court Temporarily Halts International Operation that Allegedly Deceived Consumers through False Claims of "Free Trial" Offers and Imposed Unauthorized Continuity Plans* (Nov. 28, 2018), https://www.ftc.gov/news-events/press-releases/2018/11/court-temporarily-halts-international-operation-allegedly; FTC Press Release, *At FTC's Request, Court Halts Massive "Sanctuary Belize" Real Estate Investment Scam* (Nov. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/11/ftcs-request-court-halts-massive-sanctuary-belize-real-estate; FTC Press Release, *FTC Halts Online Marketers Responsible for Deceptive "Free Trial" Offers* (July 3, 2018), https://www.ftc.gov/news-events/press-releases/2018/07/ftc-halts-online-marketers-responsible-deceptive-free-trial; FTC Press Release, *FTC Action Halts MOBE, a Massive Internet Business Coaching Scheme* (June 11, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftc-action-halts-mobe-massive-internet-business-coaching-scheme

[91] FTC Press Release, *FTC Signs Memorandum of Understanding with United Kingdom's Competition and Markets Authority to Strengthen Consumer Protection Enforcement Cooperation* (Mar. 25, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-signs-memorandum-understanding-united-kingdoms-competition. The MOU streamlines sharing investigative information and complaint data, simplifies requests for investigative assistance, aids joint law enforcement investigations, and provides strong confidentiality and data safeguards.

Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission similar enforcement powers decades ago, and provided the Consumer Product Safety Commission with permanent authority to share information with its foreign counterparts, we ask Congress to repeal the Act's sunset provision and make the SAFE WEB Act's cooperation tools a permanent part of the FTC Act.

VI. CONCLUSION

The FTC remains committed to marshalling its resources efficiently in order to effectively protect consumers and promote competition, to anticipate and respond to changes in the marketplace, and to meet current and future challenges. We look forward to continuing to work with the Subcommittee and Congress, and we would be happy to answer your questions.

Ms. SCHAKOWSKY. And thank you, Mr. Chairman, sticking within the time, too, appreciate that.

And now, Commissioner Wilson, you are recognized for 5 minutes.

STATEMENT OF CHRISTINE S. WILSON

Ms. WILSON. Chairman Schakowsky, Ranking Member Rodgers, Chairman Pallone, and Ranking Member Walden, thank you for the opportunity to testify. It is an honor to appear before you and the distinguished members of the subcommittee for the first time since I joined the Commission 8 months ago. Today I would like to highlight two areas where I respectfully believe Congress could assist the FTC in fulfilling its mission to protect consumers. First, enactment of privacy legislation, and second, clarification of the FTC's authority under Section 13(b) of the FTC Act.

With respect to privacy legislation, I agree with Chairman Simons' opening statement on this topic. I too encourage Congress to enact privacy legislation to be enforced by the FTC. Businesses need clarity and certainty regarding rules of the road in this important area. The passage of the California Consumer Privacy Act and the prospect of potentially conflicting bills in myriad States have created confusion and uncertainty in the business community. And in light of the fact that online commerce is not just national, but international in scope, I encourage Congress to include preemption in any Federal privacy legislation. Even more importantly, consumers need clarity regarding how their data is collected, used, and shared. Privacy legislation should address these concerns and could help build public trust around data collection and use.

Privacy legislation is also necessary to address the emerging gaps and sector-specific approaches created by evolving technologies. For example, HIPAA applies to medical offices but not wearables, apps, or websites like WebMD. Data protections should be based on the sensitivity of the data, not the entity or mechanism through which it is collected.

And while privacy is important, so is competition. Federal privacy legislation must be carefully crafted to maintain competition and foster innovation. GDPR may have lessons to teach us in this regard. Preliminary research indicates that GDPR may have created unintended consequences, including a decrease in investment and startups and entrenchment of dominant players in the digital advertising market. Reports also indicate that compliance with GDPR is costly and difficult for small businesses and new entrants.

U.S. legislation should seek to avoid these negative consequences. There are three other elements I believe should also be included in Federal privacy legislation: civil monetary penalties, which Congress has provided for in other statutes that are enforced by the FTC including COPPA and the Telemarketing Sales Rule; jurisdiction over nonprofits and carriers which collect, common carriers which collect significant volumes of sensitive information; and targeted, narrow APA rulemaking authority so the FTC can enact rules to supplement legislation and to permit adjustments in response to technological developments.

Turning to section 13(b) of the FTC Act, I think it is important for Congress to provide assistance through clarification of the

FTC's authority under section 13(b) of our statute. Decades of cases have established two key principles. First, the FTC may bring actions in Federal district court to obtain injunctive relief, and second, the authority to grant injunctive relief confers upon courts the full panoply of equitable remedies including equitable monetary relief.

Our ability to protect consumers relies heavily on this authority, but recent decisions have raised questions about the scope of our authority that conflict not only with long-established case law, but also with the clear intent of Congress. Earlier this year, a case in the third circuit held the FTC can't seek injunctive relief when the challenged conduct is not ongoing or imminent, but fraudsters frequently cease their unlawful conduct when they learn of impending law enforcement actions. The third circuit standard could prevent us from seeking relief in Federal district court in these circumstances, even if we can show the conduct is likely to recur based on past practices.

And another concerning development arose in the ninth circuit where a judge questioned the FTC's authority to obtain equitable monetary relief under section 13(b). But courts have long held that granting the FTC authority to seek injunctive relief also gives courts the authority to grant the full range of equitable relief. We believe this interpretation more accurately reflects congressional intent.

We thank you for your assistance, and I look forward to answering your questions.

Ms. SCHAKOWSKY. Thank you. And now we recognize Commissioner Slaughter for 5 minutes.

STATEMENT OF REBECCA KELLY SLAUGHTER

Ms. SLAUGHTER. Thank you Chair Schakowsky, Ranking Member Rodgers, Chairman Pallone and Ranking Member Walden, and distinguished members of the subcommittee for inviting us here today. I am Rebecca Kelly Slaughter and I am so pleased to be here with my colleagues on behalf of the FTC.

I want to begin by echoing Chairman Simons and most of my fellow Commissioners, and ask Congress to pass a comprehensive Federal privacy law that would give the FTC civil penalty authority, targeted APA rulemaking authority, and jurisdiction over nonprofits and common carriers. We have some of these powers in limited degree already and where we have them, we use them responsibly.

In particular, where Congress has granted us privacy related rulemaking authority, the Commission has used to put out clear rules, engage in meaningful, participatory notice and comment, and amend our rules to keep up with technological developments. For example, the FTC has rulemaking authority under COPPA. We put out an initial rule and have since adapted it to address innovations that affect children's privacy, social networking, online access via smart phone, and the availability of geolocation information. As we have made these changes, we have conducted workshops and sought input through formal notice and comment.

The rule provides clear guidance to firms on how they can comply with the law and then we enforce the law consistent with the

rule, for example, in our settlement with Musical.ly that the Chairman referenced, a company that is now known as TikTok, earlier this year. The Graham-Leach-Bliley Act also gives us some limited privacy related rulemaking authority for information held by certain financial institutions.

In March, the Commission sought comment on proposed amendments to the safeguards and privacy rules under this law. Based on our experience, we determined that the rules could benefit from modernization. We analyzed different models for strengthening them and we sought input from stakeholders regarding the best way to implement new requirements.

Just as you in Congress are doing, we at the Commission are reflecting carefully on the types of substantive privacy provisions that might best protect consumers today and in the future. The public hearings initiated by Chairman Simons have been a showcase for these debates.

I want to briefly highlight one of my own observations for your consideration. Much of our Section 5 authority and some of our privacy rules up to this point have been grounded in the principles of notice and consent. The notice and consent framework began as a sensible application of basic consumer protection principles to privacy. Tell consumers what you are doing with their data, secure consent, and keep your promises.

But in order for a notice and consent regime to be effective each element must be meaningful. Notice must give consumers information they need and can understand, and consumers must have a choice about whether to consent. Today, notice is mostly in the form of lengthy, click-through contracts. Few consumers have the time and legal training required to understand them and consumers often have no choice but to say yes to these contracts.

They must cede all control over their data to access services critical to their everyday lives. They don't have the option to turn to a competing, more privacy-protective service. In other words, when it comes to our digital lives, neither notice nor consent feels particularly meaningful today. As you consider better protections for consumer privacy, I want to encourage solutions that don't place all the burden on consumers as much as the existing framework does.

Finally, amidst the important ongoing discussions of the resources allocated to our agency, I want to conclude by highlighting what a good return on investment the FTC is for the American consumer. In fiscal year 2018, the Commission's budget was $306 million and our actions returned over $1.6 billion to consumers. So, for every dollar the American taxpayer gave to the FTC, staff returned 5. We welcomed the recent letters from Chairs Schakowsky and Pallone asking what the Commission could do with more resources and the Commission's response illustrated the good use to which we could put additional funding.

Approximately two-thirds of our budget goes to our greatest asset, staff pay and benefits. Unfortunately, our headcount has declined over the past decade even as demands on the agency have increased. The letters that we sent illustrated what we could do with an additional 50 or 75 or 100 million dollars, some of which would allow us to bring our staffing levels up to where they were

in 1982, well before the internet, and still below where they were in the 1970s.

So I look forward to working with the committee on both sides of the aisle as you think about this important legislation, and I look forward to taking your questions. Thank you.

Ms. SCHAKOWSKY. Thank you very much, and now Commissioner Phillips is recognized for his 5 minutes.

STATEMENT OF NOAH JOSHUA PHILLIPS

Mr. PHILLIPS. Thank you. Chair Schakowsky, Ranking Member Rodgers, Chairman Pallone, Ranking Member Walden, distinguished members of the subcommittee, thank you for the opportunity to appear before you today. I am honored to be back here with my fellow Commissioners to highlight the important work that the FTC and its talented staff do on behalf of American consumers. I realize that privacy is one of the main topics that we are going to talk about today, and I look forward to answering any questions that you have.

But, first, I want to highlight what the FTC has been doing in an area that is critical to all Americans, healthcare. Americans are concerned about their healthcare. All of us spend more time than we should trying to find a doctor who takes our insurance, shopping for the best prescription prices, dealing with insurers, and so on. And all too often we pay more than we should with the annual cost of healthcare accounting for nearly 18 percent of annual GDP. The FTC has focused on healthcare for decades. In my nomination process, I called for this Commission to continue that essential work and I am pleased today to report that we have.

On the competition side, the Commission has been very busy. Following the FTC's Supreme Court victory in the Actavis case, which subjected pay-for-delay settlements to antitrust scrutiny, we have worked hard to rid the market of this anticompetitive conduct. Pay-for-delay settlements delay generic entry, preventing earlier consumer access to cheaper pharmaceuticals, and forcing Americans to pay higher prices for the drugs they need. The Commission has obtained several orders prohibiting such settlements, including two this year that included the final remaining Actavis defendants.

Just weeks ago, this Commission reached a decision in its case against the generic manufacturer Impax which entered into a pay-for-delay settlement with Endo, a brand manufacturer. On a unanimous basis, we rendered the first FTC opinion on pay-for-delay settlements since the Actavis case, banning Impax from engaging in this harmful conduct. I know that stopping anticompetitive conduct and pay-for-delay settlements has also been a focus of this committee, and I appreciate the chairman, ranking member, and Congressman Rush's recognition of this important issue.

This Commission is fighting anticompetitive conduct in court. We recently obtained a Federal court judgment ordering AbbVie to pay nearly $500 million in relief to consumers overcharged for AndroGel, as a result of AbbVie's anticompetitive manipulation of our civil justice system. And as the Chairman mentioned, just weeks ago we sued Surescripts, a monopolist we allege employed illegal vertical and horizontal restraints to maintain its monopolies

over two e-prescription markets. In addition to targeting the cost of healthcare, this case addresses important competition issues like two-sided markets, network effects, and innovation harms.

Our consumer protection work on healthcare also provides results to consumers who too often get duped into buying bogus products and services, sometimes even foregoing needed care. Stopping deceptive health claims, providing guidance to business, and educating consumers continue to be top priorities for this Commission. Last month, the FTC settled with defendants charged with deceptively marketing cognitive improvement supplements using sham websites and fake clinical studies and endorsements. Our actions stopped the scam which reaped over $14 million from unsuspecting consumers.

The FTC also recently cracked down on deceptively advertised amniotic stem cell therapy which its promoters claimed could treat serious diseases including Parkinson's, MS, and heart attacks. The FTC just mailed checks over half a million dollars to victims. We also recently brought charges against defendants who claimed that their Nobetes pill could treat diabetes even after the FDA and FTC warned them that they needed scientific evidence which they didn't have. The list goes on.

We are focused on protecting consumers in the opioid crisis and have brought several actions to return money to consumers who were duped into treatments that weren't real. And as our work on the opioid crisis shows, the FTC leverages our resources and partners with other agencies to maximize our impact. Working with the FDA as we did on opioids, we jointly issued 13 warning letters to companies marketing e-liquids used in e-cigarettes in packaging that resembled kid-friendly food products like juice boxes, candy, or cookies. Like yours, our goal is to protect kids.

I hope this testimony has been helpful to you in showing how the FTC makes a daily impact on the lives of American consumers both by protecting their wallets and their health. Thank you, and I look forward to your questions.

Ms. SCHAKOWSKY. Thank you very much. And last but not least, Commissioner Chopra, it is your 5 minutes.

STATEMENT OF ROHIT CHOPRA

Mr. CHOPRA. Thank you. Chair Schakowsky, Ranking Member Rodgers, and members of the committee, thank you for holding this hearing to examine the Federal Trade Commission's role in policing digital markets against misuse and abuse of data.

Today, I want to talk about a market failure affecting families, businesses, and the labor force: terms of service, the contracts that we theoretically read and evaluate online. The FTC and Congress need to confront these take-it-or-leave-it contracts particularly when it comes to potentially unfair terms. Many terms of service consist of thousands and thousands of words written in legal jargon. According to some estimates, if Americans had to read all of these contracts it would take them approximately 250 hours per year.

Studies overwhelmingly confirm that we just don't read these terms and we are now becoming numb to companies imposing regulations that make us cede our rights and even our property. For ex-

ample, terms of service for streaming music apps have given companies access to your contacts and photos, even though it is a music app. To use certain, quote, free photo sharing apps, the maker of the apps reserves the right to use your name, likeness, and image even for commercial purposes. Other terms of service slip in language that says the company will absolutely ignore "do not track" settings in your browser.

These nonnegotiable contracts are giving firms the right to fingerprint your device, often allowing them to create a dossier on you even if you don't register for an account. These contracts aren't just claiming the right to monetize your personal information and property, they also revoke many of your legal rights and can even allow firms to change terms at any time whenever they want.

Contracts are and should be a critical foundation of commerce. They help parties bargain and put their promises on paper. But when contracts aren't negotiated, they can easily become riddled with one-sided terms, and both dominant players and unscrupulous firms can exploit their position to the detriment of fair competition.

Now the FTC has a strong tradition of restricting unfair contract terms. In the 1980s, during the Reagan administration, the FTC banned a slew of terms and consumer credit contracts including confessions of judgment where consumers waived all of their defenses in court if they were sued. The FTC found that terms like these were the product of an unequal bargain where consumers could not protect their interests.

More recently, both the FTC and Congress have cracked down on gag clauses on a bipartisan basis. Nondisparagement provisions in take-it-or-leave-it contracts that forbid us from posting truthful reviews online for products and services are now banned. This is a boon for consumers and competition. Buyers will be able to find out what others have experienced, and sellers that invest in quality in customer service will be rewarded in the market. It is time for us to own up to the fact that today's digital contracts can lead to a race to the bottom.

In addition to making use of the FTC's existing authorities, Congress should also look for ways to stop companies from exploiting their bargaining position through these contracts. For example, we can look to reforms enacted by other developed countries, such as the 2010 law in Australia that allowed consumer protection and competition authorities to enforce laws on more unfair contract terms.

I would suggest that there are two aspects that warrant our attention. First, we need to look at the circumstances that these contracts are imposed and whether one side has more power, information, or leverage. Second, we need to look at the terms themselves, particularly any one-sided terms that unreasonably favor the drafting party. It will be especially critical to closely scrutinize the terms imposed in take-it-or-leave-it contracts on entrepreneurs and small businesses like app developers and online merchants, especially when they can see their data taken away or their rights removed. This can impede fair competition and we should look closely at it.

Thank you, and I look forward to all of your questions.

Ms. SCHAKOWSKY. Thank you all. We have now concluded witness opening statements for our panel. We will now move to Member questions. Each Member will have 5 minutes to ask questions of our witnesses, and I will start by recognizing myself for 5 minutes.

So we know the FTC does not have enough resources to devote to privacy and data security enforcement. The FTC has only about a thousand employees altogether to fulfill the dual mission of competition and consumer protection which is less than what the agency had, as we heard earlier, in 1983. Of those, only about 40 people are charged with protection of privacy and security of American consumers. I can find that pretty shocking. The American people deserve more and better.

So my question is for Chairman Simons. You have said before that you believe the FTC must, quote, vigorously enforce, unquote, the laws entrusted to it. How can the FTC vigorously protect consumer privacy when it has only 30 lawyers working on behalf of the whole country?

Mr. SIMONS. Thank you, Chairman. So like you have said before, we are a small agency but we fight above our weight. So we are very aggressive with the resources that we have, but if we had more resources I guarantee that we would put those to very good use.

In terms of—one thing to keep in mind, I think particularly with respect to the legislation that you are considering, is that would significantly, no matter who you talk to, really, that would significantly expand our authority. And in particular, if that legislation is passed, there is no question that we would need very substantial increases in our resources.

And as you said in your opening statement, Madam Chairman, the U.K. authority has 500 employees dedicated to privacy and even the Irish authority has about 140. So us starting at 40 and then trying to enforce something similar to what they are enforcing with their authority, obviously, you know, shows a gap.

Ms. SCHAKOWSKY. OK, thank you.

As you had mentioned, Mr. Chairman, earlier this year we sent a letter to the FTC to get more information about how the Commission would use additional resources, and I ask unanimous consent to put that in the record. Hearing none, so ordered.

[The information appears at the conclusion of the hearing.]

Ms. SCHAKOWSKY. Your response indicated that the Commission could hire 160 more staff with $50 million in additional funding or 360 more staff with an additional $100 million funding. You also said that a hundred new attorneys focused on privacy and security would allow the FTC significantly to boost its enforcement activity and also improve the agency's ability to monitor compliance of companies already under the order.

So I am concerned about this issue of monitoring compliance with existing orders because we have all seen how, for example, Facebook continues to rampantly abuse consumer privacy despite being under an order with the Federal Trade Commission. So the question, Chairman Simons, is how does the FTC make sure that companies comply with orders that require a comprehensive program to protect privacy and security?

Mr. SIMONS. Yes, so thank you, Chairman. One of the really great things about the FTC as an institution is that it has a history of engaging in self-critical examination. And the privacy program, looking back at the FTC as a whole, is a relatively young program. So we are seeing what is happening with some of these orders.

And this also was explored at our hearings and we are taking that to heart and increasing the provisions in our model orders to beef up, for example, assessor provisions so the assessors actually have a much more fulsome role and we can get the benefit of their investigation. And also, we are creating a provision that requires certification by a senior officer in the company. And in order to make that certification, the officer is under an obligation to actually conduct an investigation and gather evidence regarding their compliance with the order.

Ms. SCHAKOWSKY. Let me ask Commissioner Chopra, does the FTC have the resources and authority necessary to effectively monitor compliance and enforce its existing orders? I am concerned that the FTC doesn't even require anyone to submit assessments to the agency after the first one.

Mr. CHOPRA. Well, of course we are using a century-old law to do much of our privacy and data security work, so obviously authority and resources will help. Of course, we are all aware no amount of resources is really going to—we don't know how much we will actually be able to tackle the vast problem that we have at hand.

So, in addition to resources, you know, bright line rules that really give clear guidance and have real teeth and accountability and especially penalties will also help us advance that mission. The more blurry it is, the more it is going to be harder to enforce, the more some firms will be able to get through loopholes and small firms will suffer.

So I also encourage you to think about not just having the FTC enforce some of these rules, but other parties as well. We need those force multipliers.

Ms. SCHAKOWSKY. Thank you. Now I yield to the ranking member of our subcommittee.

Mrs. RODGERS. Thank you, Madam Chair. And again, thank you, everyone, for your testimony here.

Chairman Simons, last month the FTC held a hearing on the FTC's approach to consumer privacy. Your remarks focused on the fact that privacy violations can cause a range of harms. I believe any Federal privacy bill should focus on protecting consumers from concrete harms. What did you learn from the hearing about specific harms that can help us craft an enforceable privacy bill?

Mr. SIMONS. Thank you, Representative. What I would say is that we learned quite a bit at those hearings. We learned that there is a widespread consensus among stakeholders in the privacy community to support the Federal privacy legislation that you are talking about, you know, you as a committee.

And they are also talking about how to—notice and comment, notice and choice has been a primary vehicle as we discussed and folks in the hearings emphasized that it really should also turn on assessments and accountability. And so, we are focused on that as well and also deidentification of data. Those are the things that

came up at the hearing and that were most recommended by a broad group of people.

Mrs. RODGERS. Great, thank you.

Commissioner Phillips, can you explain why it is important for a Federal privacy approach to be risk-based and what harms we should as Congress be protecting against?

Mr. PHILLIPS. Congressman Ranking Member, thank you for that question. The tradition of the United States since 1970 with respect to privacy has been a risk-based one. We have chosen to look at particular areas where risk is heightened, like information about kids or health information, and single out those areas for special and heightened treatment. That to me makes all the sense in the world.

This conversation that we are having about a broader consumer privacy law because it reaches broader and because it potentially applies to a far broader swath of data, some of which may raise similar kinds of risk, some of which may make less, to me means that we have to have a really serious conversation, and in particular that Congress needs to have really a serious conversation what the problems are we want to solve, what the wrongs are that we want to right.

So one of the things that I have heard today is a concern about, let's say, transparency, right. Consumers don't have the time to look over a long policy. Maybe they don't understand the legal jargon. Are there things that we can do to increase that level of awareness and maybe also provide more clarity for business? That could be a good outcome.

But I think what is critical to this debate is two things. The first, leaving aside the tools of how we solve the problem, let's agree on the problems we want to solve, say, transparency, or at least do our best to solve, and then let's think about how to build a scheme around that.

Mrs. RODGERS. As a follow up, is there a risk of delegating too much rulemaking authority to the FTC that creates uncertainty for industry, particularly the small businesses and startups?

Mr. SIMONS. Thank you again for that question. I think there is, and to me the risk exists on two levels. The first is really a basic constitutional one, which is the privacy debate is really interesting because it is one where there is a lot of general agreement on the need for something, but a lot of disagreement on the specifics.

So let me take as an example, two consumers both pushed ads as they walk by a Starbucks. One consumer might experience that as, "Great, that reminds me—I want the latte, and I want to get a dollar off." But the other consumer might say, "Hey, that is really creepy. How did you know I was there?" Those are both very reasonable interpretations of the same facts, but what they demonstrate is that different people have different tastes for privacy. So in this context, when you give broad rulemaking authority, you ask five of us or maybe even just three of us to decide what we want. That is no substitute for the democratic process.

So that is the first thing. The second thing, which you mentioned and which is really important, is that, whatever the rules are, they ought to basically remain over time. And there is a chance that, you know, issues get politicized or people have very earnest dis-

agreements and over time the rules shift. Whether you like more restrictive rules or less restrictive rules, we should all agree that having consistent rules over time makes sense.

Mrs. RODGERS. OK, thank you. I have more questions, but my time is expired. I will yield back.

Ms. SCHAKOWSKY. I now recognize Ms. Castro—Castor for 5 minutes, sorry.

Ms. CASTOR. Thank you, Madam Chair.

Chairman Simons in his testimony mentioned the recent FTC fine of $5.7 million against the video social networking app Musical.ly—it is now known as TikTok—to settle allegations that the company illegally collected information on children in violation of the Children's Online Privacy Protection Act. You said this is the largest civil penalty obtained by the FTC in a children's privacy case, but in actuality there really haven't been very many. And when you look at the circumstances here, I don't think the fine fits the crime.

You had reports that they were collecting location data on children that was discernible to people in the neighborhood. They made it very difficult to close accounts. They made it practically impossible to complain. They would not delete profiles after someone did close an account.

So, and by the way do you all know the valuation of the Chinese company that owns TikTok? ByteDance, as of November 2018, ByteDance was valued at $75 billion. That means the FTC's record-setting fine was 0.0076 percent of ByteDance's value. No CEO is going to blink an eye at a fine that inconsequential. Companies will just see small FTC fines as the cost of doing business and will continue to elevate profits over privacy, especially when it comes to our kids.

Commissioner Chopra and Commissioner Slaughter, you issued a joint statement in responses. You said, "Executives of big companies who call the shots at companies that break the law should be held accountable," I guess personally accountable, and the FTC has gone after executives when they have direct control and are calling the shots here.

Commissioner Chopra, why was it important to make that statement and is it clear the FTC has the authority to go after executives of tech companies for violating privacy laws?

Mr. CHOPRA. Well, let me just say that the FTC goes after individuals all the time, especially when it comes to small-time scammers. I do think we need to level the playing field a bit and make sure that in our investigations when it comes to privacy we are also looking at the role of individuals who made the decision that it was worth violating the law in order to profit.

So, I want to make sure that in our investigations we are investigating that and we are holding them accountable when we have clear evidence of a violation, because you are right. For some firms fines are a parking ticket and a cost of doing business and we cannot change behavior unless those penalties are painful and often that means finding out who at the top called the shots.

Ms. CASTOR. Commissioner Slaughter, I want you to answer that but I also heard you loud and clear on the privacy policies. Everyone knows that these notice and consent and privacy policies, they

are simply not working, and it is particularly egregious when it comes to children and parents.

In COPPA, they are completely inadequate to protect children's privacy, and I am worried no matter how much that we revise those notice and choice provisions it will not be sufficient and companies will find ways to around it to get to our children's data without parents fully understanding what their children are agreeing to share.

The one answer was contained maybe in the FTC's 2012 privacy report that discussed reasonable collection limitations, which I understand to mean that companies only collect data that is consistent with the context of a particular transaction or the consumer's relationship with the business. It could also include limitations on sharing, sale, retention, and usage.

Should Congress include a reasonable collection limitation section in privacy legislation going forward?

Ms. SLAUGHTER. Thank you for the question, Congresswoman. Let me try to take both of those points quickly, mindful of your time. The first is, I agree with your point and my colleague's point that fines can't be meaningless to companies. If we care about them, they need to be enough to effectively both deter specific wrongdoing by that company in the future and effectuate general deterrence.

I would like to make a clarifying point because I have heard a couple of Members talk about fines the FTC can levy. And just to be very clear, unlike some of our counterparts in Europe, we can't independently assess fines. Where we find a violation of an order or a rule, we can go to court and seek civil penalties and a court could assess penalties and then in order to avoid that process, we can negotiate with a company to reach an outcome that we think is fair and just. But those are negotiated penalties they are not levied fines, and I think that is a meaningful distinction.

And, secondly, the statement that my colleague and I released in the TikTok case did go to the question of individual accountability, making sure our investigations effectively assess where it lies if enforcement is proper, and I think we also have to think about the injunctive relief that we provide in any particular case. I think about it as sort of a multilegged stool, again how to best effectuate specific enforcement making sure this company doesn't violate the law again, and general deterrence, making sure other companies know that if they don't follow the law, the consequences will be meaningful to them.

And then——

Ms. SCHAKOWSKY. We are going to have to wrap. We are going to have to wrap it up there.

Ms. SLAUGHTER. OK, then the short version of your question about purpose limitations, I agree. I think they are really important.

Ms. CASTOR. Thank you.

Ms. SCHAKOWSKY. Thank you. The Chair now recognizes Mr. Burgess for 5 minutes.

Mr. BURGESS. Thank you. And thank you all for being here for this hearing. This is important. You are an important agency and

this subcommittee does have an important role to fulfill as far as oversight of the important agency that you represent.

So, some other Members have done a good job of articulating how for a very large company a fine simply is a cost of doing business and it is of no consequence and they are able to pick up and move on. I would like to focus just a little bit on smaller companies where the ability of the Federal Trade Commission to require compliance or even consent decrees may be a death knell for that company.

And a company that comes to mind, a case that has interested me for some time, is LabMD. Most of you were probably not on the Commission when LabMD became a thing back in the—a decade ago. And it has worked its way through the courts and, if I understand correctly, the most recent was an eleventh circuit court decision that actually put some of onus back on the FTC saying you have actually got to define these things that you want with what you want a company to comply.

But, you know, LabMD that case stands out to me as the object lesson. Here was a viable business providing a great service to the urologic practices that depended upon the handling of lab tests and pathologic specimens and now that company is gone and it is gone because of a relatively arbitrary FTC decision. And then, ultimately, the guy that pushed it all the way to the eleventh circuit, really, LabMD was not the one that was at fault.

So, Commissioner Phillips, you have talked about the healthcare issue, so assuming that you have some knowledge of, even though none of you were on the Commission when LabMD started, Chairman Simons said, you know, that the FTC—what was the—that you engage in self-critical examination, so what does your self-critical examination tell you as far as the LabMD case is concerned?

Mr. SIMONS. Congressman, thank you for the question. As you noted earlier, none of the five of us were here when the LabMD case was brought and I do want to reserve judgment on the work that others did. But I think your fundamental point is absolutely right, which is we need to think and, in fact, the statutes that we enforce command us to think very critically about remedies and the impact that they have.

Sometimes more are warranted. Sometimes less are warranted. Sometimes injunctive relief may be more important. Sometimes fines are more important. We have case law to guide us and we also have the benefit of experience. And I think critically that we need to learn from our experiences and sometimes that may militate in favor of changing what we are doing.

The Chairman mentioned earlier what we are doing on our model orders with respect to testing how well they are working. But it can cut both ways, and I think that is something we always really need to take into account.

Mr. BURGESS. Well, it is just—and when Mr. Walden was chairman of the full committee and we did have—he referenced we had representatives from Facebook here discussing things with them, a consent decree for a company the size of Facebook is inconsequential. It doesn't affect them one way or the other. The fine that Ms. Castor referenced to the company with a bottom line of 67 billion or whatever it was, that fine is inconsequential.

But for small businesses, the heavy hand of the Federal Trade Commission basically can spell the end of their business and in this case, unfortunately, it did. But even a consent decree, which your consent decrees run a number of years, for a company to have to disclose that "Yes, I want to handle your lab specimens. I want to handle your confidential medical data. Just so you know, I am under a consent decree from the Federal Trade Commission until 2032," that probably ends that company's ability to render that service. Would you agree?

Mr. PHILLIPS. I absolutely think that issues like the length of consent decrees need to be considered. Commissioner Wilson and I recently wrote in a case where the party had violated a consent decree in a really bad way, so we agreed with the penalty. But one of the things that we said together is that experience and law and the facts of the case, not necessarily by the way how it is publicly perceived, but the facts of the case and the applicable law and our experience as the agency ought to guide us in how we apply remedies.

Mr. CHOPRA. Dr. Burgess, can I add?

Mr. BURGESS. Sure.

Mr. CHOPRA. I want to agree with your sentiment on this, which is we need to avoid ever appearing that we are strong-arming small defendants and letting large ones kind of off the hook. I think there needs to be an evenness in this, because you are right that even a subpoena can be very, very costly for small firms.

So I take also away that we need to think hard about where we are allocating our resources. Are we allocating our resources to a lot of small firms or are we really thinking and gaining credibility by challenging larger firms who commit harm on a wide scale and who have the resources to litigate? Because litigation, actually, also gives much more credibility to the outcome rather than just sometimes settlements.

Mr. BURGESS. Great. I have a number of other questions. I will submit those for the record. I yield back my time.

Ms. SCHAKOWSKY. Thank you. The Chair now recognizes Representative Kelly for 5 minutes.

Ms. KELLY. Thank you, Madam Chair.

One of the key tools that FTC has used in enforcing privacy cases is deception authority, particularly when a company hasn't told the truth in its privacy policy. But there is no national law that requires companies to have a privacy policy in the first place. For instance, a recent report found that 85 percent of the apps and browser extensions in the Google Chrome Web Store didn't have a privacy policy at all.

Chairman Simons, do you believe it would be helpful to the FTC's ability to enforce the law companies were required to disclose their privacy practices?

Mr. SIMONS. I think this is something that the Congress should definitely consider in its consideration of new Federal privacy legislation. And what you have just said illustrates the imperfect nature and the lack of authority that we have, which is that our privacy program is based in large part on this deception authority that we have under Section 5, a hundred-year-old statute which was never

designed or legislated with any intent toward privacy issues that we see today obviously, so thank you for that.

Ms. KELLY. You are welcome. Even when a company has privacy policies, it practically takes a law degree to understand it or is so vague that it is meaningless to consumers. Some have suggested that it would be useful to provide consumers with clear, concise, and consistent disclosures that would make it easy to understand how companies use and share personal information.

Commissioner Chopra, do you think it would be helpful if a law required companies to label their privacy practices in a way that provided clear and consistent disclosures to consumers with wording and pictorial depictions like a 3 and a dollar sign if data was sold to a third party?

Mr. CHOPRA. Yes. I think better disclosure that is clear is always good, but on top of disclosure we have to sometimes recognize that users sometimes actually have no choice, you know, when it comes to filling out their job application, when it comes to enrolling in school, they may not have a choice.

So I want us to also think about, you know, what are the types of terms that maybe should be presumptively unlawful or where there is a higher burden to bear or where some data is just off limits, because we don't want to disguise ourselves into thinking people can meaningfully compare all the time.

Ms. KELLY. And my next question, is there something else that Congress can do to help consumers better understand how their data is used? And anyone can answer.

Mr. CHOPRA. Yes. Well, I will just add too that when it comes to deception we need to also think about dark patterns and other tactics that are being used to trick consumers into handing over their data. They use complex testing in order to nudge you. Often it is almost impossible to figure out how to close your account or delete your data and it raises very serious questions about whether it may be a violation of our deception standard, but more clarity would help.

Ms. KELLY. OK. Turning to a different subject, I wanted to talk about the interception of privacy rights and civil rights. Algorithms that profile users and target content to specific groups can too easily result in discriminatory practices against marginalized communities. For example, investigative journalists have found that employers advertise jobs exclusively to men on Facebook and also build internal algorithms that negatively ranked women for job placement.

Nearly 2 years ago, the Tech Accountability Caucus, which I chair, wrote a letter to Facebook about their discriminatory ads that allowed people to exclude housing applicants based on protected characteristics like race, gender, and sexuality. I am glad that HUD finally took action on this case and that Facebook has ceased its practice of racial affinity advertising.

Again, Commissioner Chopra, would it be helpful if Congress explicitly applied existing civil rights laws to data privacy by, for example, prohibiting discriminatory uses of personal information?

Mr. CHOPRA. Yes, this is really serious because with algorithms and machine learning they essentially allow some firms to either knowingly or unknowingly evade our antidiscrimination laws. It re-

inforces biases against rural Americans, against people of color, so us to attack what is going on behind those scenes is absolutely critical. And, you know, no algorithm is going to be free of bias and we need to make sure that the digital economy is not reinforcing biases.

Ms. KELLY. Thank you.

And, Madam Chair, I just wanted to let you know that joining me today are two young people very interested in privacy. One is from Tuesday's Children. Her father was a retired major in the Army who is now deceased. So they are listening in the back attentively to what we are going to do, so thank you and I yield back my time.

Ms. SCHAKOWSKY. Thank you. The Chair now recognizes Mr. Latta. No, is he not here? Oh, I am sorry. Mr. Walden showed up again and I am happy to recognize you for 5 minutes.

Mr. WALDEN. Thank you. I sort of snuck in from the other hearing. But thank you, Madam Chair.

And, Chairman Simons, it has been a few decades, but there was a time when the FTC, as we heard, was given broad rulemaking authority but stepped past bounds of what Congress and the public supported. This required further congressional action and new restrictions on the Commission.

In testimony submitted for this hearing, the FTC supports APA rulemaking authority for privacy legislation. Do you have any concerns with Congress delegating broad rulemaking authority to the FTC and would you support limiting that rulemaking authority to issues that cannot be foreseen by this Congress?

Mr. SIMONS. I have substantial concerns and please do not do it. Do not give us broad rulemaking authority, give us targeted rulemaking authority. Just as—because we are worried about what exactly what you have described happening again and the agency becoming politicized and we want it, so what we really want to have is we want to have the Congress——

Mr. WALDEN. Very specific.

Mr. SIMONS [continuing]. Come up with bipartisan Federal privacy legislation, have it fairly well defined, COPPA is a good model, and give us targeted rulemaking authority so that we can keep it up to date, make technical changes for developments in technology or in business methods. But please do not give us broad-based authority.

Mr. WALDEN. All right.

Mr. SIMONS. The last thing that we want to have is to have you dump that question on us, the big, broad question.

Mr. WALDEN. Yes.

Mr. SIMONS. We would rather have elected officials do that.

Mr. WALDEN. You know, and too often when we face a tough problem, we do that to agencies. We say, "Yes, we can't really figure this out, so we are just going to give you rulemaking authority. You go figure it out."

Mr. SIMONS. Yes.

Mr. WALDEN. And then when you do, we object.

Mr. SIMONS. Right. Please don't do that.

Mr. WALDEN. Because you didn't get it right, even though we couldn't figure it out. And so, I think it is, the obligation is on our shoulders to be as refined and targeted as possible.

I guess I have sort of a yes or no question for all of you. One of the issues we are wrestling with as the Energy and Commerce Committee and looking at something nationwide, do you all support a Federal preemption of existing State laws or can privacy work on a State-by-State patchwork basis?

It strikes me the internet, this, you know, some of them described with tubes and all that, right?

Mr. SIMONS. Right.

Mr. WALDEN. It actually crosses borders—who knew? And so, I am trying to figure out how it works if we don't do a nationwide law. Do you, I mean——

Mr. SIMONS. Yes, I share your concerns about the patchwork. And I think, you know, the sense of it would be that if the legislation is substantial enough——

Mr. WALDEN. Right.

Mr. SIMONS [continuing]. Then I think it makes sense to preempt. But having said that, I also think that even if you preempt, you should give enforcement authority to the State Attorneys General.

Mr. WALDEN. All right.

Ms. Wilson, what is your guidance on this?

Ms. WILSON. I agree that preemption is necessary. As you note, there are State boundaries that get crossed. There are national boundaries that get crossed. Consumers are looking for a seamless experience and, frankly, businesses need guidance. We have heard examples of bills that have conflicting provisions. For example, one State will say this is opt-in and another says it is opt-out. And businesses, literally, cannot comply with both of those State laws. And so, I believe that we do need Federal privacy legislation that contains preemption.

And I agree with Chairman Simons that the State AGs——

Mr. WALDEN. Has to be robust.

Ms. WILSON [continuing]. Who can assist in enforcing will act as a force multiplier as Commissioner Chopra noted.

Mr. WALDEN. Yes.

Mr. CHOPRA. Mr. Walden, can I——

Mr. WALDEN. Well, if I could just——

Mr. CHOPRA. Sorry. Well, go ahead.

Mr. WALDEN. Yes, we will get to you, but Ms. Slaughter?

Ms. SLAUGHTER. I am sympathetic to the desire for uniformity, consistency, clarity, and predictability in a national law. I would be concerned about a Federal law that lowered standards that already exist in the States, so I think the appropriateness of preemption is best evaluated in terms of whether a Federal law meets or exceeds the level of protections that States can provide and whether it allows them the opportunity to fill any gaps that may remain after a Federal law is developed.

Mr. WALDEN. OK.

Mr. Phillips?

Mr. PHILLIPS. Thank you, Congressman, or thank you, Chairman—Ranking Member.

Mr. WALDEN. Chairman in exile.

Mr. PHILLIPS. Yep. No, no, no. I hope I pulled that one back quickly enough.

Mr. WALDEN. You are all right.

Mr. PHILLIPS. I think preemption is essential for a few reasons. The first is to give businesses the clarity that they need and the second is to meet the expectation that we have all been talking about, about aligning consumer understanding with what is going on. The more variability that you have, the less transparency, the less consumer power.

Mr. WALDEN. Right.

Mr. PHILLIPS. The other thing we need to keep in mind is competition. Having multiple laws means multiple different compliance costs.

Mr. WALDEN. Right.

Mr. PHILLIPS. That is harder for smaller firms, easier for big ones. Another thing to keep in mind—I will finish very quickly—is international interoperability. We have to consider our national interests in cross-border data flows.

And, finally, with respect to establishing just a floor that is a model that we have in HIPAA, and I think Congress ought to take a very careful look at how the HIPAA model works because the studies show that State HIPAA laws have inhibited the roll-out of electronic medical record use. They have inhibited innovation, and reduction of costs in the medical field, and startups are struggling with this.

I may be wrong, I may be right. People can take different views. But I think that is a very good area to look at the data, see what is going on, and see how it would apply here.

Mr. WALDEN. Madam Chair, with your indulgence, could our final Commissioner weigh in? My time is expired.

Mr. CHOPRA. Yes, I just want to make sure I caution you that preemption can also have a lot of unintended consequences. In Illinois, for example, there is a biometric law. There are other laws that may not, may complement and not conflict. My own experience in this relates to the mortgage meltdown where broad preemption of State mortgage laws clearly wreaked more havoc because States that wanted to provide certain safeguards to their homeowners had that robbed of them.

So I think it is important that we just make sure we are not making things worse and at the same time——

Mr. WALDEN. That is a good point.

Mr. CHOPRA [continuing]. Promoting lots of beneficial entry into the marketplace.

Mr. WALDEN. Yes, I go back to my Jamie Dimon quote that said you can overregulate to the point only the bigs can afford to comply, and now you have snuffed out competition. So, this is why it is hard. We want to get it right for our consumers, we don't want to snuff out innovation. So, thanks for all the work you are doing there in helping us.

And, Madam Chair, thanks for your indulgence in this and for having this hearing.

Ms. SCHAKOWSKY. I now recognize the chairman of the full committee, Mr. Pallone.

Mr. PALLONE. Thank you, Madam Chair.

Companies are collecting more data than ever and using it in ways that most consumers would never imagine. If I download a flashlight app, for example, it shouldn't need my precise location and it definitely shouldn't then go and sell that information to the highest bidder, all without my permission. Yet the FTC does not have the authority to enact rules that could establish reasonable limits on uses of data and no comprehensive Federal law currently exists.

So I want to start with Chairman Simons. In your testimony you support Federal privacy and data security legislation, which I appreciate, but some have argued that the FTC has not done enough with the authority it has been given. How can Congress be sure that the FTC will aggressively protect consumers if given new authority?

Mr. SIMONS. My mantra is vigorous enforcement, so as long as I am the Chairman we are going to vigorously enforce. I will have to say also that we have brought lots of cases in this area where we can. We have brought about, when you consider the full range of privacy authority that we have ranging from Section 5 to the FCRA to COPPA to Do Not Call to CAN–SPAM, we have brought over 500 cases.

So I would say we have been pretty active, but our authority is limited as you describe, and so, if we get more authority, we will need more resources.

Mr. PALLONE. OK. Let me go to Commissioner Chopra.

How important is it that comprehensive privacy legislation set reasonable limits on the way the data can be used such as through data minimization and restrictions on selling or sharing data beyond the consumers' reasonable expectations?

Mr. CHOPRA. Yes, these bright line standards will also be easier to enforce. We will not have to go through as much extended investigation and also it will make it easier for businesses. So I think when you are being affirmative about what is inbounds and out of bounds, that is better.

Mr. PALLONE. OK. I am going to go back to the Chairman again. Although privacy is an important issue, it is obviously not the only critical consumer protection issue within the FTC's jurisdiction. And topping the list of the FTC's nearly 3 million complaints were imposter scams, where a scammer pretends to be from the IRS or the Social Security Administration or another trusted organization to get people to turn over money or personal information.

Consumers reported losing nearly $488 million in these kinds of scams last year. So let me ask you, Chairman, consumer education is important but the burden should not fall on consumers to stop fraud. So what is the FTC doing to stop these scams and prevent them from becoming even more common? I mean these are the things that I hear about on regular basis from constituents, particularly seniors.

Mr. SIMONS. Right. Thank you for that question. There is no single fix to this pernicious scam, but so we try to implement a multipronged approach. We have substantial law enforcement to stop these things from occurring where we can find and sue the perpetrators. But we really do think that enforcement along with

consumer and business education, consumer guidance and business guidance are important and so we tackle this on a two-front basis.

Mr. PALLONE. All right.

Mr. PHILLIPS. Chairman, may I just add briefly to that?

Mr. PALLONE. Sure, go ahead.

Mr. PHILLIPS. I really want to thank you for that question, in particular for the following reason. You have been talking recently a lot about the need for resources. It is important, especially as the headlines focus on particular issues with which we deal also to consider the ones like scams that don't always grab the headlines. That work has always been and should remain really important work that we do.

So when you think about resource questions, I would encourage you to consider all the work that all the different bureaus at that FTC does and how important they collectively are to the national interest.

Mr. SIMONS. Yes, can I just say one other thing? The FTC is a very busy place. People generally are not sitting down and doing nothing. They are all very highly active. They are all very highly productive. And so, if we are going to devote more resources, for example, to privacy, we would probably have to take them away from something like potentially going after some of these scams.

Mr. PALLONE. Unless we have more resources, but, believe me, I am the last person who thinks that Federal agencies or the people that work there don't do anything. I am constantly reminding people that they work very hard because oftentimes people think that government and politicians don't do anything, but, in fact, we all work very hard, or most of us do.

So thank you again. Thank you, Madam Chair.

Ms. SCHAKOWSKY. Thank you, the gentleman yields back. And now I recognize Mr. Guthrie.

Mr. GUTHRIE. Thank you, Madam Chair, for the recognition. Thank you all for being here. And I will agree with my friend, The Chairman, that people in our agencies do work very hard and sometimes we need to make sure we give them the right direction and how we as the policymakers would like for them to work.

And one thing that I have been concerned about as we move forward and we need to move forward on a privacy bill, I am for that, but the one thing I am concerned, I think Mr. Phillips mentioned that some of the smaller companies can't deal with it as much as some of the bigger companies.

And so, I have talked about innovation and whatever the healthcare or anything here, kind of my common theme is how do we keep this innovation that is moving forward. And so, Chairman Simons, I believe any Federal bill must ensure all companies no matter the size of their compliance department can continue to innovate and compete. And what do you think about this concern and how should we consider this drafting legislation?

Mr. SIMONS. So this is a really critical concern, thank you for raising it.

Mr. GUTHRIE. And any of the others can answer too. I called and said your name, but others can answer if they would like to, to how we can make sure people can compete, but go ahead.

Mr. SIMONS. Yes, so what I was going to say is, so we have a dual mission, consumer protection including privacy and competition, so we are sensitive, really, to both. And the thing that—one of the things that we are very concerned about is the situation where, so, for example, if you require opt-in for certain kinds of information or maybe even all the information, that makes it much easier for high-tech platforms that are consumer-facing to get that opt-in. And so, for a new company or a small company, it is very difficult to get that kind of opt-in and access to that data.

So that might constitute a very significant disadvantage for the small companies and the new entrants and cause a huge advantage for the existing high-tech platforms. And, in fact, I understand that a high-level competition official from the European Union is concerned about this because he thinks that business is being pushed by the GDPR to Google and Facebook.

Mr. GUTHRIE. That was my next question. So concerned about what GDPR, what I have heard what you just said and how we guard against that. So I mean, just what you just kind of said, if Mr. Phillips or anybody else would like to talk about that because that was my next question in light of what we know about GDPR what should we be concerned about. And you just started going into that, so I wanted to make sure we finish that and if some others would like to talk to it as well.

Mr. PHILLIPS. Thank you. Congressman, I think this is such a critical question. The important thing to remember, while a lot of this debate focuses on a few very large firms, the use, the collection, the monetization of data is endemic in the economy. It is everywhere. It is lots of little firms too. And I think the most essential thing to do is to go and consult with those firms and ask them, "Hey, how would this look for you?" You know, we want the small businesses to higher coders not lawyers. If you have five people and one of them is a lawyer, maybe that is not good for innovation and competition. So I think consulting with them, asking how the rules apply to them, not just the big firms, is critical.

Mr. CHOPRA. Yes, I would love to add just two points here. I think you are right that we have to think hard about competition. And one of the things I worry a lot about it is we are seeing a real slowdown in small business/new business formation even in the digital economy.

You know, many venture capitalists, many new firms that are starting are saying, you know, "The big guys actually have already taken all the key data. We are never going to catch up. We now have to create our business maybe just to sell to them." That can really distort innovation in our country and I am really, I am increasingly worried that our lack of attention to this issue is deterring lots of entrepreneurs from wanting to challenge those incumbents. So we need to think hard about that.

With respect to GDPR, GDPR uses essentially a principles-based regulatory scheme. So on one hand that might create some flexibility. On the other hand, it can also lead to uncertainty. And with bright line rules that actually is easier for everyone to comply with rather than huge complexity that only the largest firms can lawyer up to figure out.

Mr. GUTHRIE. OK. I am going to switch gears real quick about something in my home, one of my home industries which is Kentucky bourbon. And we have heard from a lot of our distillers and people who ship that counterfeiting distilled spirits is on the rise both domestically and abroad. I only have a few seconds. So this is a problem because consumers aren't getting the goods they purchased and counterfeit spirits can pose a serious hazard.

Chairman Simons, can you speak to the FTC's ability to monitor and regulate these sales? I know they are through websites and it is difficult to do.

Mr. SIMONS. Yes, so this type of thing is obviously of concern to us. It is a deception. You know, it is counterfeiting, like you said. The primary agencies that have jurisdiction over this, I think, are actually the Treasury Department and the DOJ who actually has criminal authority. So I think this is more of an issue for those agencies.

Mr. GUTHRIE. OK. Well, thank you very much and my time is expired and I yield back.

Ms. SCHAKOWSKY. Now the Chair recognizes Mr. O'Halleran for 5 minutes.

Mr. O'HALLERAN. Thank you, Madam Chair.

Good afternoon. Now I see it is afternoon and thank you for appearing before us today. Your role in protecting consumers and competition is critical, particularly in a world where innovation and technology is rapidly advancing and consumers are faced with navigating the maze of new technological developments and regulations. Like my colleagues on this committee, I look forward to learning more from all of you about this work.

This week, the FTC is celebrating National Small Business Week—I thank you for doing that—acknowledging the important contributions of small businesses, their owners, and in our communities. As you may know, the 1st district of Arizona is home to many small businesses, it is mostly a rural district, including mom and pop shops. Many of these business owners are located in those types of rural areas throughout the country.

A critical role of the FTC is to provide consumer education and conduct and outreach. These efforts include providing practical and plain language guidance on many issues for small business owners, many of whom are not up to the speed that the larger businesses are. In fact, the FTC has conducted several roundtables over the past couple of years to educate small business owners on various matters including cybersecurity.

It is my understanding that the Commission heard many concerns from small business owners about data security including concerns pertaining to the mobile phones and cloud devices. I would like to hear more about these initiatives and programs for small business owners and specifically how the FTC is tailoring its educational and outreach campaigns to those small businesses in rural areas and how to expand it also as you move forward.

I have two questions. I want to start with Mr. Simons and then anybody can jump in. I believe these small business outreach initiatives are important for the FTC to continue. In your view, what more can the FTC do to build upon the work of these small businesses' initiatives moving forward?

And the second question is, as you know, Congress is currently considering proposals to include in legislation on a range of issues impacting consumer privacy and data security. As the FTC considers enforcement actions against corporations who violate privacy laws, how does the FTC consider enforcement actions against small businesses versus those against larger companies? Mr. Simons?

Mr. SIMONS. Thank you, Congressman. So let me start the last question first. So we have a standard for data security that is a reasonableness standard. It is not a one-size-fits-all and we are very nervous about anyone who would suggest a one-size-fits-all standard, because as you can imagine a huge company can afford to spend hundreds of millions of dollars on its data security because it has so much volume over which to spread it and the cost per unit is going to be trivial, right. But if you make small businesses do those same types of data security measures, they will be out of business. They wouldn't even come close to making money.

So it is really important that we do this reasonableness standard, we consider how small the business is, how costly it is to provide data security, and what kind of data the company has. If it is not very sensitive then you don't worry so much about the security, or you don't worry as much and what you would expect them to do in terms of data security measures would be a lot smaller.

In terms of the outreach to businesses and consumers, this is a critical thing that we do. And people suggest to me sometimes that maybe you should divert some resources from that to doing more law enforcement, more litigation, for example, and I think that is a mistake. We really need to have this consumer outreach and outreach to the business community and we could do more of it if we had more resources.

Mr. O'HALLERAN. Thank you, anybody else?

Ms. SLAUGHTER. Thank you, Congressman. I would just add that I think there are elements of what are in the rules and the laws that are important; there are also important questions about the application of prosecutorial discretion. When we see particular cases, I think it is incumbent upon us to consider what is the company that we are considering. How big is it? What is its compliance opportunities or costs, and take that seriously in making sure that our cases and, more importantly, our remedies are carefully tailored to the particular defendants we have in front of us; it is not a one-size-fits-all approach.

Mr. O'HALLERAN. Thank you. And, you know, talking about smaller businesses for a second, I appreciate what you said about the issue, but they also fit into the entire security chain and privacy chain and how they blend into that is important for the overall security of the process. So it is kind of, I worry about both ways, so.

Mr. SIMONS. It is a balance you have to strike. You know, it is like most things in life, there are tradeoffs.

Mr. O'HALLERAN. Thank you, Madam Chair, and I yield.

Ms. SCHAKOWSKY. The Chair now recognizes Mr. Bucshon for 5 minutes.

Mr. BUCSHON. Thank you, Madam Chairwoman.

Health information is some of the most valuable data that is out there. It is very private, very personal, but also very valuable to

people. And I was a healthcare provider before. So, Chairman Simons, one of the focuses that I will have on a privacy bill, how we address health information not covered by HIPAA and how does the Commission deal with this type of health information now and how should we be thinking through this issue when fitness trackers and other health apps are very popular and becoming more popular?

Mr. SIMONS. Yes, I mean if you are talking about the same data that is covered by HIPAA and you are talking about, you know, it is really, it is sensitive data, you have to think about treating it in a similar manner. And one of the things that I think is the real advantage of the Federal privacy legislation that you were considering is that it would be broad-based and not cabined to particular types of information. And so, I think that makes things easier to deal with.

Mr. BUCSHON. Yes, because, you know, there is going to—I mean there is real-time glucose monitoring for diabetics, and people may not want people to know that they are diabetic and that information could be out there, or your blood pressure could be high and people may not know. I mean it is going to be real important that we figure how we protect that type of information, I think.

Mr. SIMONS. Yes, I agree.

Mr. BUCSHON. Yes.

Ms. Wilson, do you have any comments? Commissioner Wilson?

Ms. WILSON. I agree that the Federal Trade Commission has long applied a risk-based approach to the evaluation of privacy and the more sensitive the information, the greater the protections it deserves. We have taken the same approach with Federal legislation, children's information in COPPA, health information in HIPAA.

The gaps that you are mentioning concern me. Emerging technologies change the landscape and some of this very sensitive information is not currently covered under Federal legislation. We can get at it through our Section 5 authority, but having guidance at the Federal level would be very useful, and so greater authority in that area would help protect this information more.

Mr. BUCSHON. Yes, because I mean we have been talking about, you know, how you have to click "agree" if you want to get a certain account, right, and that is probably true with devices that now monitor your health, right. And so that will be an area we have to look at too. People, you know, broadly as you mentioned that people should know if they put on a certain device that it may very well transmit health information to someone, and it may be in the paperwork and you may just not know.

I will give you a second.

Ms. WILSON. So I completely agree. I think consumers are able to make decisions that are in their own best interest if they have information about the choices that they have. But there is a lot of consumer confusion right now. There is a lack of clarity about what is being done with their data. Greater transparency is an imperative.

Mr. BUCSHON. Yes, and even when they know maybe that their health information is going to be transmitted, they still should have some coverage for the privacy of that like under HIPAA.

Mr. CHOPRA. I just wanted to add, something that makes this even harder is with artificial intelligence and machine learning. Even if we don't hand over our health information, companies may know our health information based on what we are searching in terms of our symptoms, geolocation of where we are going. So that is going to make it really difficult when formulas and algorithms are determined and it may even know our health conditions even if they have not been formally diagnosed.

Mr. BUCSHON. Yes, I mean if you have your phone on you and you show up at an oncologist's office that tells people kind of——

Mr. CHOPRA. You have cancer.

Mr. BUCSHON. Yes, and I don't know how we protect that.

Commissioner Phillips, do you have any comments on this?

Mr. PHILLIPS. I said earlier that one of the things that Congress has done over time is it has looked at areas of greater levels of risk and I think this is an area that deserves strong consideration, and I think I agree with all my colleagues when I say that. The one thing I would add is that I do think it is important not just to consider the what in terms of HIPAA, but how HIPAA has worked. HIPAA, the studies show, has sometimes prevented what can be really pro-competitive and pro-consumer technology.

Mr. BUCSHON. Yes, yes.

Mr. PHILLIPS. You know, you fill out a form every time you go to the doctor's office, every single doctor, and the doctors can't talk to each other so you have to repeat your symptoms to——

Mr. BUCSHON. Oh, I am very well aware of that problem.

Mr. PHILLIPS. And so, I do think when we talk about HIPAA we ought to think about how it is working and how it is not working.

Mr. BUCSHON. OK, thank you all, I yield back.

Ms. SCHAKOWSKY. I now recognize Congresswoman Blunt Rochester.

Ms. BLUNT ROCHESTER. Thank you, Madam Chairwoman, and thank you all for your testimonies. First, before I get into my questions about privacy and data security, I want to ask you about our seniors who face scams especially through exploited practices like gift cards. And today I am introducing the Stop Senior Scams Act with my friend and colleague, Mr. Walberg of Michigan, who is across the aisle. And this bill is a House companion to a bill introduced by Senators Casey and Moran earlier this year.

I know you and your staff are working with the Senators and I look forward to working with you further as we consider this bill on the House side. And, Commissioners, I just wanted to ask briefly if you are seeing a lot of this like on the rise in terms of the scams for seniors with these gift cards? If you could just briefly and then we will jump into the other questions.

Mr. SIMONS. This is a big issue for us. You know, we are focused very much and have a high priority for scams dealing with the senior community. And we put out, we do a whole bunch of different things in terms of education. We put out guidance that, you know, if it is a gift card it is only supposed to be for gifts, right.

We have a program what we call Pass it On, which is an effort to, as one of my colleagues said, be a force multiplier. It is to get people in the seniors' community to help other people in the seniors

community avoid these types of things. So this is something we are very focused on and outreach is very important in this regard.

Ms. BLUNT ROCHESTER. Great. I look forward to working with you on this. I want to shift to the privacy and data questions and I want to turn our attention to something that came up earlier when Representative Kelly was speaking. I think it was Commissioner Chopra who talked about dark patterns and that it is gaining a lot of notoriety.

And I really wanted to kind of focus on this, because for those who don't know what it is, and I am going to ask you, Commissioner Chopra, to actually share how you would describe this. How I have it is, it is a pattern, or for—a dark pattern is a website or app design that is intentionally deceptive in order to push users into content, products, or even participate in data collection activities without their informed consent. And I can bet everybody in this room has been a victim to this. And even, ironically, if you Google dark patterns, later you will probably be affected by this.

In the privacy space, many of my colleagues have touched on similar issues as it impacts consumers, children, and social media, but most recently even the IRS Free File had a connection to dark patterns. People seeking income-based assistance in filing their taxes were potentially steered unsuspectingly to products that were neither part of the IRS program or were free. And entities like Facebook we hear are—that they are affected by it, but there are even more out there.

So if you could talk a little bit about this practice. And then if you could also talk about what we in Congress should be doing to address it.

Mr. CHOPRA. Sure. And, Congresswoman, I am not an expert on it, but my general understanding is that using various sorts of testing and tactics, firms can nudge consumers into choosing certain things or deterring them. And one of the, I believe the researcher who coined the term also uses the term "roach motel,"——

Ms. BLUNT ROCHESTER. Yes.

Mr. CHOPRA [continuing]. Which is that you can check in, create an account but it is impossible to get out. And one of the things that I hope that we can really modernize some of our analytical tools, use different types of economics including behavioral economics, to understand how consumers actually can be harmed by this.

I am not positive, to be honest I am happy to answer questions for the record about whether our deception authority here is enough, but it is very troubling.

Ms. BLUNT ROCHESTER. Yes, I was actually going to ask about deception authority, but you said you are not sure.

One of the other questions, as the more that you all talked, when you talked about artificial intelligence, machine learning, geolearning, one of the questions I really have is from a workforce perspective. Are we in government, do we have the skills, the capabilities, the training to be able to be a step ahead of what is upon us now? I would love to—yes, Commissioner Wilson?

Ms. WILSON. So I think this is one of the great things about the Federal Trade Commission. We do have a history of engaging in competition and consumer protection R&D. And Chairman Simons, last summer, announced the competition and consumer protection

hearings for the 21st century, and we have held hearings with dozens and dozens and hundreds of participants and comments focusing on things like AI and machine learning and algorithms and how these affect consumers and the kinds of harms that can be created.

And so, I think we are continuing to learn and to move up the learning curve and I think with that learning we can begin to identify precisely the resources that we need to fulfill our mission of protecting consumers.

Ms. BLUNT ROCHESTER. My time has run out, but I had so many questions as well about behavioral research and study, but thank you so much for your testimony.

Ms. SCHAKOWSKY. And of course all of the questions can be submitted for the record. We hope our witnesses will reply.

And now let me recognize—oh, Mr. Hudson has arrived. You have 5 minutes.

Mr. HUDSON. I thank the chairwoman and thank you to all the Commissioners for your time today.

Chairman Simons, as you have heard today, we are committed to protecting small businesses and promoting innovation. Some other agencies are using or considering regulatory sandboxes for new innovations. Can you explain this concept and whether you believe we should consider a similar approach for privacy regulations?

Mr. SIMONS. So the regulatory sandbox as I understand it—and thank you for the question, Congressman—is a situation where small businesses would be able to—play is not the right, I mean that is the analogy—but to get started. And so, for example, people have proposed that for small businesses that they wouldn't have to comply with like, for example, maybe a Federal privacy legislation that you pass in the coming months until they get to a certain size.

And to be honest, I have thoughts positive and negative about that. So the positive is it cuts down, clearly, on the cost of getting into business and maybe allows people to grow that would never get off the ground. On the other hand, if the privacy legislation you pass really is protecting people, you know, small businesses can get a lot of sensitive information and you really worry about that.

Mr. HUDSON. I appreciate that answer.

Mr. PHILLIPS. Congressman.

Mr. HUDSON. Commissioner Phillips, do you support the use of regulatory sandboxes and what are the barriers you see to doing something similar like this?

Mr. PHILLIPS. So I think it is something very much worthy of consideration, but I want to add something and this may be my mistake, but I have a slightly different understanding of how at least internationally some of these regulatory sandboxes at working.

My understanding is and it may be how you structure it, it isn't necessarily just a shield for liability for small businesses, it is an opportunity maybe where the law is gray or something that is close to the line where under the supervision of the regulator the business can undertake an innovative thing that might be legally questionable. This is something they are pioneering in the United King-

dom right now on privacy. It has been utilized in the financial space.

I do think consistent with and as a parent of small children allowing your kids to play in the sandbox that supervision is key, but I do think it is an opportunity to test, you know, where are there maybe some pro-competitive impacts to the conduct. The Chairman is a hundred percent right that small businesses can present risks just like big businesses can. It is a question of how you structure it. But there are some, really, examples out there that I think you should consider.

Mr. HUDSON. Great. I appreciate that.

Chairman Simons, as you know there are many other industries across the United States that are subject to various privacy laws. Some of the most familiar are the Health Insurance Portability and Accountability Act for the healthcare industry; Graham-Leach-Bliley for financial services. Do you believe the FTC would have to exercise concurrent jurisdiction with the other Federal agencies to implement a national privacy law and, if so, how would you recommend we do that?

Mr. SIMONS. Well, I think it depends on what you pass, right, so you could pass a law that says yes or says no to that question. And also I think it depends on, you know, how much, you know, what you put in the law in terms of whether as a result of that whether you want to make, you know, what is now covered by HIPAA covered by your new privacy legislation or some of these other things, whether you want to fold that in or not. So it is kind of hard to say in a vacuum.

Mr. HUDSON. But if we follow that example, you know, how would we implement that, the HIPAA example?

Mr. SIMONS. Oh, so you mean if you had these jurisdictions?

Mr. HUDSON. As far as agencies going to work together.

Mr. SIMONS. We would just have to coordinate to make sure we don't step on each other. I mean we have lots of that. Like, for example, the FDA and the FTC are regulating, you know, drugs in different ways, but it is the same drug, you know, so that kind of coordination is common.

Mr. HUDSON. Got you.

Bouncing back to Commissioner Phillips, a difficult piece of this privacy discussion is the sharing of consumer data and downstream misuse. We know sharing information offers great benefits, but once a company shares that information, we see misuse from companies two or three steps down the supply chain.

How does the Commission approach this issue and do you have any recommendations on this point for a Federal bill?

Mr. SIMONS. I think looking at the supply chain and understanding the full scope of companies involved in the use of data, which is breathtaking, right, in its scope, is critical. We need to understand how the data are being used. We also though need to understand that the point at which the consumer interacts with the company is a very critical point for transparency and things like that.

Mr. HUDSON. Thank you.

And, Madam Chairman, my time is about up, so I will yield back. I thank the Commissioners.

Ms. SCHAKOWSKY. The gentleman yields back.

I understand there is some desire by the panel of witnesses for a short break. I understand that, so let's make a maximum of 5 minutes and let—and then they will come back, OK. Or maybe Members as well would like to take that moment.

[Recess.]

Ms. SCHAKOWSKY. The committee hearing will resume and I will recognize for 5 minutes, Mr. Luján.

Mr. LUJÁN. Thank you, Madam Chair.

Commissioner Slaughter, rapid advancements in technology have transformed the way that companies use personal data. In just over a decade, we have moved from a world of desktop computers to one where each of us has devices always on, it seems always collecting data about everything we do and everywhere that we go. It is vital that the FTC keep current on new technology and train its staff on emerging consumer protection issues.

Despite the often-technical nature of privacy and security matters, the FTC has only five full-time staffers classified as technologists. How do technologists help the staff attorneys on privacy and data security cases?

Ms. SLAUGHTER. Thank you for the question, Congressman. Technologists are extremely important. When we need to understand the material with which we are working in any particular case, and the more highly technical the field, the more highly technical the practices that we are investigating, the more we can benefit from the experience of a technologist. I think, I routinely try to rack my brain to think of cases we have encountered not just in the privacy and data security area, but across our mission in competition and consumer protection that don't involve some technological element and it is very difficult for me to think of any.

Mr. LUJÁN. What role do technologists play in helping identify cases where someone might have violated the law?

Ms. SLAUGHTER. I think they can play an extremely valuable role. I mean we, our case identification comes from consumer complaints, it comes from press stories, it comes from experience of staff who identify issues, and technologists can apply a level of expertise to picking out technological-specific issues that might not necessarily occur to an attorney independently.

Mr. LUJÁN. Commissioner Slaughter, do you know how many of the five technologists the FTC has work on privacy and data security enforcement?

Ms. SLAUGHTER. I am not actually entirely sure how to answer that direct question, but to the extent that you are suggesting that five technologists is not a lot for the scope of the work that we are obligated to do in privacy and data security, I agree that we could benefit from a lot more technological expertise.

Mr. LUJÁN. Chairman Simons, do you know how many of the five technologists work on privacy and data security enforcement?

Mr. SIMONS. My understanding is that one——

Mr. LUJÁN. Your microphone, please.

Mr. SIMONS. My understanding is that at one point or another they all do.

Mr. LUJÁN. Are there enough technologists for the FTC to do their work?

Mr. SIMONS. We could certainly use more. And what we do with them, actually, is so they do original research. They also educate our lawyers, so it is kind of a bit of a force multiplier. And in addition, they serve another very important function is where we don't have internal resources sufficient to help us with our cases, they identify experts for us outside the agency who we can then hire on a contract basis.

Mr. LUJÁN. And one specific question to all the Commissioners, do you agree that it would help the FTC's enforcement activities if there were more technologists working directly with staff attorneys?

Mr. SIMONS. Yes.

Mr. LUJÁN. Yes?

Ms. WILSON. Yes.

Ms. SLAUGHTER. Yes. We put an economist on every case that we consider both competition and consumer protection. I think we could benefit from technologists too.

Mr. PHILLIPS. Congressman, yes. But I just want to reiterate a point that the Chairman made, which is the use of outside experts. The thing about technology is, there is a lot of it, and a lot of it is different. If you bring someone on permanently, they may have expertise in a given area, but if you use the money to hire on a case-by-case basis, you can be more tailored, more efficient, and look at more different kinds of technology.

Mr. LUJÁN. Just as long as those experts don't have a conflict of interest with the space you are playing in?

Mr. PHILLIPS. Oh, of course you want to avoid conflict of interest in hiring outside folks.

Mr. LONG. Commissioner Chopra?

Mr. CHOPRA. Yes, I agree with Commissioner Slaughter completely.

Mr. LUJÁN. Appreciate that.

Mr. Chairman, the last several FTC Chairs have appointed a chief technologist to advise the Commissioners on significant policy issues involving new technologies. You have now been in charge of the agency for more than a year at a time when the FTC is addressing some of the most significant privacy and data security issues in the agency's history, and yet you have chosen not to appoint a chief technologist to assist you on the Commission. Why not?

Mr. SIMONS. Well, that was one of the first things I looked at upon becoming Chairman. And what struck me right out of the box was that the chief technologist is appended to the Chairman's Office in a kind of unusual way in the organizational chart. The chief technologist had no direct reports, no infrastructure for him or her, no staff. They weren't directly connected to the staff of the Bureau of Consumer Protection or the Bureau of Competition, and so that struck me as an odd organizational structure.

And so, I talked to people in the Bureau of Competition and Bureau of Consumer Protection. The Bureau of Consumer Protection has its own technologist staff called the Office of Technology Research and Investigation. That is where the five technologists are housed. That group works extremely well with the people in the

Bureau of Consumer Protection and they were going to be very upset if I moved those people out.

I was thinking about creating a Bureau of Technology. So rather than do that we created a technology task force in the Bureau of Competition which is going to have a technology fellow. And I have transferred the FTE from the chief technology officer to the technology task force in the Bureau of Competition so we have more boots on the ground in terms of dealing with these investigations that we are conducting.

Mr. LUJÁN. But still very clear that more technologists would be of beneficiary, especially with the numbers that I shared earlier, 500 million, 148 million, 87 million just to name three examples.

Mr. SIMONS. Yes.

Mr. LUJÁN. Thank you for the time, Madam Chair.

Ms. SCHAKOWSKY. Thank you and now I recognize Mr. Gianforte.

Mr. GIANFORTE. Thank you, Madam Chair.

And thank you for being here for this important topic. Last week, we had another subcommittee hearing on robocalls. And Montanans are getting bombarded with robocalls and they are sick and tired of them. One constituent in my district got a call from her little brother. Unfortunately, her little brother had died of a heroin overdose a couple of months earlier. This was a terrible situation for her and nobody should really have to go through this. This has to end.

I am just curious, Mr. Chairman, what is the Commission doing to stop robocalls like these?

Mr. SIMONS. Yes, thank you for that question. And, first of all, this is an issue for domestic tranquility in my own household. This is, to me, when I was coming into office this was probably the most important thing at least in that my wife was telling me about and then lots of other people too, and it is such an incredible inconvenience. And worse than that it is not just an inconvenience, it often leads to fraud.

So our Do Not Call rule has been overcome by technological advances and so we have to find other ways to do it and we are proceeding on multiple fronts. We still continue to bring significant enforcement actions to shut these people down who are doing these robocalls; we coordinate with the FCC. And the other thing that we would really like help from you in the Congress is to give us jurisdiction over common carriers, because there are some common carriers that cater to this robocall traffic, particularly the traffic that originates from overseas. And if we had the ability to go after these common carriers, we could, I think, put a significant dent in these robocalls.

Mr. GIANFORTE. OK. We have the situation where these robocallers, if that is a noun, masquerade as local numbers.

Mr. SIMONS. Yes.

Mr. GIANFORTE. Would this common carrier authority allow you to go after those individuals and that behavior?

Mr. SIMONS. Yes, in the sense that we could identify the carriers that are facilitating the robocallers and just stop them from, like in the case of the foreign ones stop them from entering the U.S. telephone network at the outset.

Ms. SLAUGHTER. Can I just jump in there, Congressman, and add that——

Mr. GIANFORTE. Yes, Commissioner.

Ms. SLAUGHTER [continuing]. I think the Chairman referenced how technological innovations have overtaken us and you mentioned this neighborhood spoofing problem. I think it is also worth Congress considering whether not just enforcement should be applicable to common carriers, but whether there should be more onus placed on the cell phone carriers in the first place and more responsibility placed on them to stop some of this traffic that goes over their network, I think, in the first instance even before you consider the enforcement on the back end.

Mr. GIANFORTE. OK, thank you.

Commissioner Phillips, my understanding is that when the FTC seeks to recover ill-gotten gains from any entity that has violated FTC competition rules, the Commission seeks to recover the profits from the unlawful act. Is that correct and can you briefly explain how the Commission calculates ill-gotten gains?

Mr. PHILLIPS. Do you mean in the competition context?

Mr. GIANFORTE. Yes.

Mr. PHILLIPS. Yes, and thank you for that clarification. So let me give a little context and then give you the answer. The, traditionally, three things that we have considered in the context of whether to pursue ill-gotten gains disgorgement in a competition case include whether the rule is clear, so whether it is serving that deterrent function that we want it to; second, we consider is there a reasonable basis to calculate it, and I will talk about how we have and, in fact, how it applied in a case that I mentioned earlier; and third, we consider whether there are other ways of remediating the issue, so civil lawsuits and things like that also being out there.

In the AbbVie case, which is a good example, what we did a lot of, you know, hard economic or like a lot of measurement to determine what they were making relative to what they would have been making without the anticompetitive conduct. In that case it was a sham litigation keeping drugs off the market. And so that is the differential at which we look, you know, what you made and what you would have made without doing the thing you weren't supposed to do.

Mr. GIANFORTE. OK, thank you.

Chairman Simons, I am concerned with legislating for the sake of legislating and seeking to solve a problem that may not exist. I believe any Federal privacy bill must focus on specific harms. You talked to this earlier. Can you elaborate a little bit on why it is so important we focus on privacy harms to consumers in our attempt to legislate in this area?

Mr. SIMONS. I mean I agree with you completely. Thank you for that question that if it ain't broke, don't fix it. And if you are going to, you know, you only want to create legislation for things that are causing problems and you have a fix for it. So in the privacy sector, however, the harm, I think, is very tricky and that is one of the reasons that we—and also with data security one of the reasons we need civil penalty authority, because it is hard to measure in any kind of precise, quantitative way if you are talking about, you know, a monetary relief.

And so, because of that factor you really need to do civil penalties and you need to think about is there a harm like a privacy invasion or something like that which is not monetarily—you can't—it is hard to quantify but it is still a harm. People, it still bothers people. It still, it can lead to other problems.

Mr. GIANFORTE. OK, thank you.

On that I yield back, Madam Chair.

Ms. SCHAKOWSKY. Thank you and I now recognize Mr. Soto for 5 minutes.

Mr. SOTO. Thank you, Chairwoman.

I think it is safe to say at this point that the internet is integral to our daily lives and has been for over 20 years, which is why it is so shocking that there hasn't been a single law to regulate internet privacy directly during that time and beforehand. So it is my belief that the biggest threat to internet integrity is congressional inaction. We see a patchwork of statutes, 1914, FTC Act creating your Commission, who would have thought that President Woodrow Wilson would have such an influence on the internet? 1986, Electronic Communications Privacy Act to protect communications; also 1986, Computer Fraud and Abuse Act. 1998, Children's Online Privacy Act, which was referenced by Congresswoman Castor. 2003, the CAN–SPAM Act to protect us against unsolicited emails.

Most of these predate the internet and pretty much all of them were created when dial-up was still the form of getting on the internet. So I just want to make a statement to say that you know, you all are charged with a really impossible task. You have to interpret these isolated moonstones to come up with this comprehensive privacy regime because Congress hasn't given you direction on it.

So thank you for doing what is nearly impossible to do, which is regulate privacy without laws to directly do that. Even the courts have filled in the gap with Carpenter v. U.S. establishing cell phone privacy.

So, Madam Chairwoman, I hope that we will out of this committee be able to develop some key protections, making sure that companies have a duty of care, a duty to protect civil rights, and a duty to protect privacy. And that the penalties will be sufficient so it is more costly to pay for a breach than it is to pay for sufficient cybersecurity investments.

Second, I hope that we establish that Americans have a right to control their information, a right to stop the use of their information if they choose so, and if they do, companies should have a right to charge for their services. And third, waivers should be put in plain language. I want to get out how we are determining damages. We heard a little bit of that discussion before.

I have read in the paper that there may be a fine against Facebook between 3 to 5 billion dollars. Chairman Simon, what is the total amount of that fine?

Mr. SIMONS. Oh, I am sorry, Congressman, but I can't talk about an ongoing nonpublic investigation.

Mr. SOTO. What factors do you generally utilize in determining those types of damages?

Mr. SIMONS. So you would look at the prior conduct, the culpability, the ability to pay, and the deterrent effect.

Mr. SOTO. Commissioner Chopra, if it was at the upper end of $5 billion, do you think that would be a sufficient deterrent for the activities complained of?

Mr. CHOPRA. I think it is not appropriate to comment on that. Obviously, deterrence is important. When it comes to violations of our rules, violations of our orders, nothing can be the cost of doing business.

Mr. SOTO. Turning to the TikTok settlement that Congresswoman Castor talked about, Chairman Simon, what were the factors utilized in determining that fine?

Mr. SIMONS. I believe the ones I articulated.

Mr. SOTO. And——

Mr. SIMONS. And the other thing too is that you know, this is a negotiation that resulted in a settlement. And we also have to take into account what the likely outcome would have been in court and if we couldn't have done better in court, then it makes sense to settle. And that is one of the issues that we face kind of generally is that historically the civil penalty awards have been quite low and so one of the things we are thinking about is a way to get them generally raised on average.

Mr. SOTO. So that is something else this committee has to work on then is to make sure that the civil penalties are a sufficient deterrent.

Commissioner Slaughter, was the TikTok settlement a sufficient deterrent for on the behavior complained of?

Ms. SLAUGHTER. The statement that Commissioner Chopra and I put out in connection with that settlement explained that the investigation and, really, most of the negotiation of how to resolve that case took place before this slate of Commissioners was constituted. And it is very difficult for us, I think as a general matter, to look back without having been part of a conversation to discuss it, so we were focusing on in the future whether it is—not whether—that it is important that our investigations, including of large companies, really ask all the questions that we need to determine where liability properly lies.

Mr. SOTO. Thank you for that. I want to turn to identity theft. We see in our notes 444,000 complaints of identity theft. Chairman Simons, do you know the cost to the economy or the loss to the economy that identity theft on the internet poses currently?

Mr. SIMONS. I think the average is about $150 per person.

Mr. SOTO. And so, do you have an overall figure for that or do we have to multiply it by 330 million?

Mr. SIMONS. I don't other than it is quite large.

Mr. SOTO. OK, thanks. And I yield back.

Ms. SCHAKOWSKY. The gentleman yields back and now I ask Mr. Carter for his 5 minutes.

Mr. CARTER. Thank you, Madam Chair.

And, Mr. Simons and Commissioners, thank you for being here. This is an extremely important subject as you well know and we in Congress are depending on you and we are relying on you to help us through this because it is something that we want to get right. And it is certainly something that our constituents and the citizens of our country need to have right and to be done by right.

Mr. Simons, I want to ask you, where in the current law, where does the FTC's ability to enforce privacy or where does it end? I mean, you know, I have heard you say before that the FTC is the cop on the beat when it comes to privacy and I understand that. But, you know, where does your authority end at this point or under current law?

Mr. SIMONS. Right. Thank you for that question, Congressman. So, our general Section 5 authority comes from that hundred-year-old statute which was not designed, for sure, to deal with this kind of issue, so I credit my predecessors at the FTC for basically inventing a privacy program out of Section 5. I think they did a terrific job with the material they had available on them and it is based largely on a deception authority.

So we started out by saying you should have a privacy policy at your company and then if you divert from it then that is a deception and we can hold you accountable. And then we expanded that to include, for example, things that look like privacy torts at common law and we cover those under unfairness. But in terms of the general privacy authority, not including FCRA or COPPA or whatever, this is really it and it is pretty narrow.

Mr. CARTER. So you would agree that something more would help?

Mr. SIMONS. Yes. I mean that is why we are encouraging the Congress to adopt privacy legislation.

Mr. CARTER. OK, and not only for that reason, but I mean, if we look at the other laws that are being proposed like in California and Europe, you know, here we have a situation where we really need something to be preemptive particularly in the case of what is being offered in California.

I mean it is very important that the Private Right of Action that is being proposed in California that that would be an additional punishment on top of the FTC action as I understand it. And certainly, we don't need plaintiffs' attorneys to be involved in this. We need the FTC to be the cop on the beat as you describe them.

Mr. SIMONS. Yes. I think what I have said before is that we should be the enforcer of that legislation that you are considering and you should allow the State Attorneys General to enforce as well, just as they do in lots of other areas in conjunction with us. They are a terrific partner and I would strongly recommend that.

Mr. CARTER. So you have the ability and you do take action on fining certain—and posing financial penalties. How do you come about—how do you come up with that? I mean how do you determine how much that is?

Mr. SIMONS. Well, it depends on the case that is involved. And just to be clear, we don't actually have any fining authority ourselves like our counterparts do in Europe. We would have to go to court, actually, to get a fine paid unless it was pursuant to a consent settlement.

Mr. CARTER. OK, so you have to go to court, so you have to justify it in court as to why you think it should be that much?

Mr. SIMONS. Yes, so that is the limiting factor in all of this. Anytime you are thinking about a settlement, if the settlement gets to a point where you say to yourself, "Gee, we probably cannot do nearly as well as this, or maybe we could do just about as well as

this in litigation, but the litigation has lots of risks," so when you get to that point then you really should settle. I mean that is the appropriate thing to do. Otherwise, if you are just going to go to court and irrespective of the settlement, then that really becomes almost unethical or potentially harassment.

Mr. CARTER. So when the financial penalty is imposed where does it go?

Mr. SIMONS. So specifically for a civil penalty that would go to the Treasury, so that would be for an order violation or like in COPPA we have civil penalty authority. That would apply there. With respect to our 13(b) authority where we go in and get injunctive relief and we get consumer redress that gets disbursed to the consumers.

Mr. CARTER. OK. Well, you know, again I would look at this as being a tremendous opportunity for us as Members of Congress to work in a bipartisan fashion to come up with something that would benefit everyone and certainly, you know, would benefit citizens. And if I get input of any kind, certainly privacy is one of the things that is on top of the list. I mean constituents are consistently telling me, you know, we need this. We need this. And this is something, you know, we don't want to stifle innovation or anything, but we do need our privacy protected.

So thank you very much and thank all of you for your work on this, and I yield back.

Ms. SCHAKOWSKY. The gentleman yields back and now I recognize Mr. McNerney, patient Mr. McNerney, for 5 minutes.

Mr. MCNERNEY. Well, I thank the chairlady. And one of the problems of being last is that all the questions I wanted to ask have already been asked, so forgive me if I am repetitive here.

But Pete Olson, my Republican colleague Pete Olson, and I are cochairs of the AI Caucus, and one of the areas that I am interested in is algorithmic biasing and data biasing. And we have discussed that a little bit already, but I know that the FTC has had a couple of hearings focused on AI and there was a report entitled, "Big Data: A Tool for Inclusion or Exclusion."

Chairman, what steps is the FTC taking today to protect consumers from potential harm and bias in AI algorithms and——

Mr. SIMONS. This is something we look at carefully and is a priority for us. We had a recent case, actually, involving a company that does background screening using algorithms and the algorithms improperly associated people with criminal records. So we got them to fix their algorithms, this is a form of AI. So this is something we are looking at. It is real.

Mr. MCNERNEY. Well, you don't have any authority over algorithms and decision making on lethal use of force, say, in law enforcement, do you?

Mr. SIMONS. I don't think so. I mean anything that is criminal we wouldn't have jurisdiction over.

Mr. MCNERNEY. OK. Is the agency developing any guidance or educational tools to help address the problem?

Mr. SIMONS. I think we have business outreach that suggests that businesses think about these types of issues as they are, you know, and they look for biases and the results of their algorithms in AI.

Mr. MCNERNEY. Well, I know that Mr. Luján asked a similar question regarding the importance of technologists. Is the Commission planning on hiring technologists in the AI field specifically for bias?

Mr. SIMONS. We don't have a specific plan to do that unless we get more resources. But what we do in the interim is we use our existing technologists on our staff to do outreach to the technology community and to talk to experts, to have conferences, and to help them educate our staff.

Mr. MCNERNEY. But are there any other AI potential harms that the FTC is considering besides biasing?

Mr. SIMONS. There probably are, but I just, you know, I can't think of it, as I said.

Mr. MCNERNEY. Anyone else on the Commission?

Mr. CHOPRA. Sure, Congressman. One other area we think about with respect to artificial intelligence is in our work to enforce laws against anticompetitive conduct. Sometimes algorithms and AI can help online sellers collude on price. It can lead to, you know, other anticompetitive conduct, and we are thinking about this across the agency.

Mr. SIMONS. Yes, one thing about that that is interesting is if AI allows companies to tacitly collude more easily that might be a justification for more aggressive merger enforcement in industries where that is occurring.

Mr. MCNERNEY. Chairman, does the Commission have the authority to structure civil penalties to be meaningful to large companies without devastating small companies? Do you have that authority?

Mr. SIMONS. Yes. We have flexibility in that regard.

Mr. MCNERNEY. OK, so you don't need any congressional legislation or anything like that.

Mr. SIMONS. Not to deal with the flexibility issue.

Mr. MCNERNEY. Thank you. I understand the agency held 13 hearings to evaluate practices of both Competition and Consumer Protection Bureaus. I know you are still in the process of receiving comments, but I do have a series of questions about these hearings especially because I know these hearings took up a significant amount of the resources and the Commission has limited resources.

Can you give me the top three takeaways from these hearings? What is the basis of what you have learned?

Mr. SIMONS. So one of the things we learned is that merger retrospectives are really important and we got a lot of good testimony on that and that is something we really need. And if we got more resources that is one of the things we would do, and in particular merger retrospectives as relate to vertical mergers. That was highly recommended.I don't think really that is the literature, the literature on merger retrospectives is much greater on horizontal and is much less on the vertical merger side. So that was one.

With respect to privacy and data security, we got a lot of feedback that we really do need civil penalty authority, that we need targeted rulemaking, and that we need jurisdiction over common carriers and nonprofits.

Mr. MCNERNEY. I mean a little schizophrenic about rulemaking, I mean you want the rulemaking to be targeted——

Mr. SIMONS. Yes.

Mr. MCNERNEY [continuing]. But you don't want it to put you in a bind as well, so I understand that.

Mr. SIMONS. No, so we would like—at least my view is that these privacy issues involve very serious and significant societal and cultural value judgments, and those should be made to the greatest extent possible by elected officials and not people who are unelected. So our view is that—my view is that you should make those judgments.

And we are happy to help you make them. We are happy to work with you. We are happy to provide analysis of the tradeoffs that any particular piece of legislation may present. But, you know, at the end of the day, our view is that Congress should do that and we should have authority to do rulemaking that allows us to keep the whatever you pass up-to-date and consistent with new technology and new business methods.

Mr. MCNERNEY. Thank you. Thank you, Chairwoman.

Ms. SCHAKOWSKY. The gentleman yields back. And, Mr. Cárdenas, you are recognized for 5 minutes.

Mr. CÁRDENAS. Thank you very much. Thank you very much, Madam Chairwoman, for having this important hearing with the FTC. My question to the FTC is that in 2018 FTC cases resulted in a total of about $2.3 billion in refunds for consumers who lost money to frauds and other unfair or deceptive practices. I commend you for doing that especially when you look in light of the overall budget for FTC is about $300 million per annum. But recent Federal court decisions put the FTC's power to get compensation for consumers at a serious risk, particularly in cases where the company has stopped violating the law. For example, my question is can one of you explain how these decisions limit the FTC's authority under Section 13(b) of the FTC Act?

Ms. WILSON. Sure, so this is a critical issue, thank you for raising it, and it is why I addressed it in my opening statement that the issue is that the third circuit has recently put in place a standard that would enable us to go after conduct in courts only if the conduct is ongoing or imminent.

And so, if in the course of an investigation a defendant halts the conduct that we are challenging, say, a fraudster stops defrauding people or an advertiser suspends dubious advertising claims, then we are unable to go after that conduct under the third circuit standard unless we are able to show that it is imminent. So even if the fraudster has engaged in fraud in the past but is not doing it at this moment, unless we can prove that it is imminent, we can't reach it.

And this is a serious question that has been raised about the scope of our authority. We believe that this flies against a long line of cases saying otherwise, but we would appreciate clarification from Congress on the scope of our 13(b) authority.

Mr. CÁRDENAS. OK, thank you.

Chairman Simons, how serious of an issue are these decisions for the FTC's enforcement of Section 5?

Mr. SIMONS. So if they were to become the law of the land, so to speak, this would be highly problematic for us. I think it would basically destroy our fraud program. We wouldn't be able to recover consumer redress——

Mr. CÁRDENAS. Fraud as in protecting the consumers, protecting the people of America.

Mr. SIMONS. Yes, like you referenced to whatever it was, the 2.3 billion or whatever, we wouldn't be able to recover that if these cases became law.

Mr. CÁRDENAS. OK. What do these cases do to the FTC's ability to make consumers whole?

Mr. SIMONS. They really just take it away.

Mr. CÁRDENAS. OK, so basically the FTC in this as what we are talking about at the moment is actually helping the American people set something right, so the FTC is actually a part of that.

Mr. SIMONS. Yes, absolutely.

Mr. CÁRDENAS. OK, so Congress could write clarifying law, right, that that is what Congress hopefully should and will do.

Mr. SIMONS. Yes, we would love for you to do that.

Mr. CÁRDENAS. Yes. Hopefully I can talk to some congressional Members and we will do that.

Mr. PHILLIPS. Congressman, could I add just one thing to that?

Mr. CÁRDENAS. Yes, please.

Mr. PHILLIPS. And I absolutely agree with my colleagues that clarifying longstanding precedent on the impact of 13(b) is essential. I want to add another thing. Next year the SAFE WEB Act is going to expire. This is an essential tool that we use to work with our partners abroad to do cross-border consumer protection including privacy enforcement. I think it is a no-brainer and you ought to consider that as well.

Mr. CÁRDENAS. Thank you.

Mr. Chopra, do you have anything to add to that?

Mr. CHOPRA. I agree with my colleagues completely.

Mr. CÁRDENAS. Good. That is great. Appointed by Democrat and Republicans and you all agree on this issue. Good, good, good, good.

So when it comes to made in the USA, my time is limited so I will cut to the point and the question. I am concerned that the FTC settled on some cases for no money without so much as an admission of liability and some defendants effectively cheated consumers and got away with little more than lying about products being made in America. That obviously has a value on the streets of America. I personally love to buy made in America products.

But for someone to actually lie about it when they make the product, put it out to market, and then for there not to be any way of them having to pay a price for doing that for duping the American people, Chairman Simons, where are we at with that?

Mr. SIMONS. Yes, so historically for decades that has been the approach that the Commission has pursued in these made in the USA cases. They have only got injunctive relief. But we are now going to hold a workshop and look at what we need to do in terms of beefing up our remedies.

Mr. CÁRDENAS. So hopefully FTC will come out with a more aggressive, appropriately aggressive stance when it comes to people lying about made in America.

Mr. SIMONS. That may very well be the outcome of the workshop.

Mr. CHOPRA. Just like in privacy legislation where you are thinking about civil penalties to deter this conduct, Congress gave the FTC the power to activate penalties for made in USA violations 25 years ago. We have not yet turned that switch on and I hope that we can explore and potentially turn that switch on, because we need to deter this and put a stop to it, because this absolutely harms every single honest manufacturer in America who makes goods here at home.

Mr. CÁRDENAS. Yes.

Ms. WILSON. If I could add one point, the cases that have been reported on this issue were decided and settled between staff and the parties before this slate of Commissioners arrived, and as Chairman Simons noted in his statement, when the settlements were first announced. We do intend to look at this policy going forward, but the decision of many of the commissioners was to not upset the work that had already been done by staff in the previous slate of commissioners, but to look at this going forward.

Mr. CÁRDENAS. Madam Chair, if I can have 5 seconds.

If someone is willing to lie boldface about made in America, I as a grandparent am afraid that that product might have cheated on other things such as chemicals and other matters that might be involved in the net product that might end up in the hands of my grandchildren or any other American family. Thank you very much, Madam Chair, yield back.

Ms. SCHAKOWSKY. Mr. Walberg, I am going to call on you, 1 second.

Let me just point out to the committee that every single Member on both sides of the aisle have shown up to this hearing. That doesn't happen all the time, and I think it is a tribute to the issue, but also to our commissioners. So I want to thank you.

Mr. Walberg is waiving on to our committee. We are happy to have you, and you have 5 minutes.

Mr. WALBERG. Thank you, Madam Chairwoman, and thank you for consenting to waiving me on this subcommittee. And while I am not on the subcommittee, certainly I have an interest in being a member of the Energy and Commerce Committee. I appreciate you allowing me this opportunity.

Thank you, each of you, for being here today as well. You have a big job and we wish you well and we hope that we can be supporters and fellow laborers in making the difference.

I wanted to come here today to ask questions about a topic very important to me and my constituents, and that is scams against targeting our Nation's seniors. Michigan seniors, in my case, have spent a lifetime working to save for financially secure retirements. In the digital age, scams targeting seniors and their hard-earned money are growing in number and sophistication, and safeguarding vulnerable seniors needs to be a top priority. I am one. It is important to me. Today, Representative Blunt Rochester, who I believe mentioned this already, she and I will be introducing legislation, the Stop Senior Scams Act, to help prevent fraudsters from targeting seniors with prepaid or gift card scams.

While the committee is working on legislation to address annoying robocalls and that scam our seniors into giving away their sav-

ings or personal information, gift card scams are another way fraudsters target seniors. Companies like Target or Wal-Mart are on the front lines against these scams, and their ability to educate their employees with best practices and training to recognize the signs of scam can make a huge difference in stopping a scammer. The Stop Senior Scams Act would create a forum at the Federal Trade Commission to communicate about best practices like this.

And so, Chairman Simons, I would like to ask you if you could please talk about what the Commission is doing to prevent frauds and scams against seniors and how legislation like this Stop Senior Scams Act would align with the FTC's consumer protection mission.

Mr. SIMONS. Thank you, Congressman. So this is a multipronged approach at the FTC. We engage in strenuous efforts going after these specific scams that target seniors. We have what is very important, I think, and very effective is a program of outreach to the senior community and we have a specific program that was designed called Pass It On, where we try to kind of essentially deputize senior citizens to help their fellow senior citizens avoid scams. So they are talking about it in their local communities and it is on top of mind and they know what to watch out for. And your legislation, you know, it sounds like I couldn't agree more with the goals of it and I would be happy to work with you on it.

Mr. PHILLIPS. Congressman.

Mr. WALBERG. Yes.

Mr. PHILLIPS. If I could just add one thing, since we are here in a public hearing and hopefully the public is paying attention. What I want to say to American consumers about this critical issue to which you and Congresswoman Rochester have devoted such important attention, if a business tells you that you need to pay with a gift card, it could very well be a scam and people need to be on the lookout for that. We are going to be doing our jobs, but it is also important that we communicate to the public.

Mr. SIMONS. Yes, the real thing here is, if somebody wants you to pay with a gift card and that is what you are telling you, it is probably a scam. Gift cards are for gifts, they are not for forms of payment.

Mr. WALBERG. From your lips to seniors' ears then.

Mr. SIMONS. Yes.

Mr. WALBERG. What developments, Chairman Simons, have there been in financial scams affecting seniors and how can the Commission help stop these scams from spreading to larger groups of seniors?

Mr. SIMONS. So these things are just evolving continually and it is, you know, you stop one type of scam and another type of scam arises. And so, the trick for us is to stay on our toes, pay attention to what is going on, and move to each succeeding new scam.

And one of the things that enables us to do that is our Consumer Sentinel database which is an incredible tool for law enforcement and particularly for dealing with scams. It has an enormous number of complaints in it and shared by us with the local State authorities across the country, and it is a great asset.

Mr. WALBERG. OK, any other comments?

Mr. CHOPRA. I hope that we also start paying closer attention to how seniors are scammed online. More and more seniors are also participating in the digital economy, also connecting with family, and many, especially those who suffer from diminished capacity can be particularly at risk.

Mr. WALBERG. Well, I appreciate that. It is a big issue and it is not going away and it is expanding. So our efforts together will be very helpful for the constituents I represent and those all over this great country.

So, Madam Chairwoman, thank you for allowing me this time.

Ms. SCHAKOWSKY. Thank you, Mr. Walberg.

I just want to—I am surprised none of you mentioned that the FTC does do these scam workshops. I don't know if they are everywhere, but we really have this amazing one in the Chicago area, Brad Schneider and I. And the FTC organized it, but brought in a representative of the Attorney General, various other State agencies, and it was spectacular. It was chaired by the Federal Trade Commission.

So I don't know if it is in Mr. Walberg's district, but I would suggest that you ask for one of those. It was really good.

Mr. SIMONS. And we would be thrilled to do it.

Ms. SCHAKOWSKY. OK. And so, Mr. Rush was here earlier, but we welcome him back for his 5 minutes of questions. Mr. Rush?

Mr. RUSH. Yes, I want to thank you, Madam Chair.

It has been one of the—the means of committees that—those that pull us in a different direction, and some of them when they come in, they come in right before it is over. So I know those who sit patiently were not overwhelmed with enthusiasm when they saw me walk through the door, but it is the way this place operates.

So I want to thank you, Madam Chair, for holding this hearing. And I want to begin by asking unanimous consent to offer into the record an October 2018 letter from the AMA. So I ask unanimous consent.

Ms. SCHAKOWSKY. Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. RUSH. All right. I want to begin by saying that the FTC is one of my most favorite agencies in the Federal Government. I worked very closely with the FTC, particularly when I chaired this subcommittee some years ago and did some really good work with the FTC.

But I want to—Chairman Simons, on October 26, '18, the AMA sent you a letter encouraging the FTC to monitor insulin pricing and market competition out of increasing concerns that the rapid rise on the price of insulin may be attributed to anticompetitiveness rather than research and development. If, Mr. Chairman, as the letter alleges, if this is true, how would the FTC respond? And the second part on the question is, have you investigated the claims made in the AMA letter?

Mr. SIMONS. Thank you for the question, Congressman. So I can't respond specifically to any nonpublic investigation that is going on, but I will say this. We are very focused on pricing in the pharmaceutical sector. We monitor pricing on a monthly basis over a wide range of drugs to see if there are any anomalies like the one you

just described, and we look specifically to see if they are caused by anticompetitive activity. And if they are, this is a source of case generation for us, so these are a source of investigations. So that is the type of, exactly the type of thing that we could look at.

Mr. RUSH. Is there any one of the commissioners that might want to respond?

Mr. CHOPRA. Yes. I think the situation we see with insulin is it is not isolated. It really, we see it all over. I believe in the case of insulin it is really only three players—Eli Lilly, Nova Nordisk, Sanofi—who really have all the volume. The original patent was sold for $3 generations ago.

We see a lot of challenges across the pharmaceutical market with respect to abuse of intellectual property. My colleagues talked about some of the work there. But we have to use all of our tools to crack down on anticompetitive conduct and the fewer and fewer players we have in the market that raises more concerns.

And it just bugs me that some of these treatments are old. Insulin is not dramatically different than it used to be and the fact that people can't get it affordably and are skipping out on it——

Mr. RUSH. Right.

Mr. CHOPRA [continuing]. It is literally killing them.

Mr. RUSH. Anybody else?

Mr. Phillips, I understand you had some nice things to say about me earlier. I really appreciate it. It came across my desk.

Mr. PHILLIPS. Absolutely, Congressman. In my opening statement I talked about the work that we are doing on a bipartisan basis at the FTC to help deal with the cost of healthcare, on the competition side included a lot of really good work over the last year, a half a billion judgment, an important antitrust case filed weeks ago, a decision on pay-for-delay settlements, which I know have been very important to you, that we issued 5-nothing, just a few weeks ago. So I want you to know from me that the cost of healthcare and rooting out anticompetitive conduct in the healthcare industry is and will remain a focus for all of us.

Mr. RUSH. Well, thank you.

Madam Chair, thank you so very much for your indulgence and I yield back the balance of my time.

Ms. SCHAKOWSKY. Thank you, Mr. Rush.

Just a little bit of business left. I request unanimous consent to enter the following testimony or letters, other information into the record. Without objection, so ordered.

A letter for the record, Oversight of the Federal Trade Commission: Strengthening Protection for—oh, OK; a letter from the Electronic Privacy Information Center; a letter from Consumer Bankers Association; a letter from the Internet Association; a letter from the National Association of Federally-Insured Credit Unions; and a letter from the Confidentiality Coalition.

[The information appears at the conclusion of the hearing.][1]

And, finally, I want to thank our ranking member. I want to thank the staff on both sides of the aisle. And I especially want to

[1] The Electronic Privacy Information Center letter has been retained in committee files and also is available at https://docs.house.gov/meetings/IF/IF17/20190508/109415/HHRG-116-IF17-20190508-SD004.pdf.

thank our witnesses, members of the Federal Trade Commission, for coming here today.

I remind Members that pursuant to committee rules they have 10 business days to submit additional questions for the record to be answered by the witnesses who have appeared. I would ask each witness to respond promptly to any such requests that you may receive.

And at this time, the subcommittee is adjourned.

[Whereupon, at 1:26 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

FRANK PALLONE, JR., NEW JERSEY
CHAIRMAN

GREG WALDEN, OREGON
RANKING MEMBER

ONE HUNDRED SIXTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

March 20, 2019

Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chairman Simons:

With the start of the 116th Congress, the Committee has resumed its traditional role of oversight to ensure that the agencies under its jurisdiction are acting in the best interest of the public and consistent with their legislative authority. The Federal Trade Commission (FTC) plays a critical role in protecting U.S. consumers from a wide variety of unfair and deceptive practices, including protecting consumers' data privacy and security. As described below, we are writing today to better understand the resources that the FTC needs to fulfill its important consumer protection mission and meet the challenges posed by rapid changes in technology.

A series of recent high-profile privacy incidents have caused significant concern to consumers and this Committee. In the past year alone, consumers have seen privacy scandals from some of the country's largest technology companies, including the Cambridge Analytica/Facebook data leak;[1] two bugs in Google+ that allowed third-party app developers to access millions of users' personal information;[2] and an Amazon Alexa that shared a recording of

---

[1] *87 Million Facebook Users to Find Out If Their Personal Data Was Breached*, ABC News (Apr. 9, 2018) (abcnews.go.com/US/87-million-facebook-users-find-personal-data-breached/story?id=54334187).

[2] Electronic Frontier Foundation, *The Google+ Bug Is More About the Cover-Up Than the Crime* (Oct. 11, 2019) (www.eff.org/deeplinks/2018/10/google-bug-more-about-cover-crime); *Google Reveals New Security Bug Affecting More Than 52 Million Users*, Washington Post (Dec. 10, 2018) (www.washingtonpost.com/technology/2018/12/10/google-reveals-new-security-bug-affecting-more-than-million-users/?utm_term=.3499d20fe0c1).

a couple's conversation without permission.[3] Then, just last month, Google disclosed that it's Nest Secure alarm system secretly included a microphone that it never disclosed to consumers.[4] Additionally, massive data breaches at companies such as Equifax[5] and Marriott[6] have exposed the sensitive personal information of hundreds of millions of consumers. For every high-profile case, there are many more that do not get attention in the press and therefore may not be prioritized by the FTC. Nevertheless, consumers may face significant harm from these less well-known privacy and data security incidents.

Given these significant concerns, the Committee's Subcommittee on Consumer Protection and Commerce recently held a hearing entitled "*Protecting Consumer Privacy in the Era of Big Data.*" Members of the Subcommittee believe that legislation is needed to protect the privacy of our constituents and that the FTC must have additional resources and authority to meet these 21st century challenges.

We are writing to you to learn how the Commission could use additional budgetary resources to better protect consumer privacy. We would appreciate your responses to the following questions and respectfully request that you provide a complete written response no later than April 3, 2019:

1. What resources would the FTC require to dramatically boost its enforcement activity with respect to privacy and data security? How would the FTC deploy new resources if it were to receive an additional $50 million for consumer protection and privacy? How about an additional $75 million? How about an additional $100 million? As part of your responses, please estimate the number of additional investigations and enforcement actions the FTC would likely be able to pursue.

2. If Congress were to direct the FTC to hire technologists to aid in case development, enforcement, rulemaking and/or policy recommendations, what resources would the FTC need to fulfill its consumer protection mission and how would the agency deploy those new resources? Specifically, please describe the number of employees the agency would need, their roles and responsibilities, and

---

[3] *Is Alexa Listening? Amazon Echo Sent Out Recording of Couple's Conversation*, New York Times (May 25, 2018) (www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html?rref=collection%2Ftimestopic%2FPrivacy).

[4] *Users alarmed by undisclosed microphone in Nest Security System*, Ars Technica (Feb. 20, 2019) (arstechnica.com/gadgets/2019/02/googles-nest-security-system-shipped-with-a-secret-microphone/).

[5] *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, New York Times (Sept. 7, 2017) (www.nytimes.com/2017/09/07/business/equifax-cyberattack.html).

[6] *Marriott Hacking Exposes Data of Up to 500 Million Guests*, New York Times (Nov. 30, 2018) (www.nytimes.com/2018/11/30/business/marriott-data-breach.html).

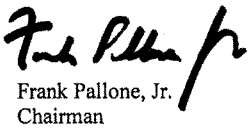
how the FTC would use these resources to further its consumer protection mission.

3. If the FTC received notice-and-comment rulemaking authority with respect to privacy and data security, would the FTC require additional resources to develop and update new rules without detracting from the agency's enforcement activity? If so, what resources would the FTC require?

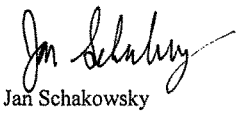
4. What would the FTC be able to accomplish with 100 new attorneys focused on privacy and data security that it cannot do with current resources?

We appreciate your willingness to appear before the Committee when called upon and hope we can continue to count on you to be responsive to all Congressional inquiries in a timely fashion. If you have any questions regarding this inquiry, please contact Lisa Goldman of the Committee staff at (202) 225-2927.

Sincerely,



Frank Pallone, Jr.
Chairman



Jan Schakowsky
Chair
Subcommittee on Consumer
Protection and Commerce

OFFICE OF
THE CHAIRMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

April 1, 2019

The Honorable Jan Schakowsky
Chair
Subcommittee on Consumer Protection and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chair Schakowsky:

Thank you for your March 20, 2019 letter requesting information about how the Commission would use additional resources to protect consumer privacy. The Commission has long exercised the authority Congress has given it under various statutes to address consumer privacy harms arising from new technologies and business practices. We have brought hundreds of privacy and data security cases, hosted about 70 workshops, and issued approximately 50 reports.

However, we need additional tools and resources to better protect consumers' privacy. I support federal privacy and data security legislation that would allow us to obtain civil penalties for violations, conduct rulemaking under the Administrative Procedure Act ("APA"), and exercise jurisdiction over common carriers and non-profits.

- First, as to civil penalties, the Commission can only obtain civil penalties against first-time violators for cases involving the Children's Online Privacy Protection Rule ("COPPA") or the Fair Credit Reporting Act ("FCRA"). To help ensure effective deterrence, we have urged Congress to enact legislation to allow us to seek civil penalties for data security and privacy violations in appropriate circumstances.
- Second, the ability to issue rules under the APA would enable us to better keep up with business and technological changes. Where we currently have APA rulemaking authority, we have used it judiciously. For example, in 2013, the FTC used its APA rulemaking authority to amend the COPPA Rule to address new business models, including social media and collection of geolocation information, that did not exist when the initial 2000 Rule was promulgated.
- Finally, any privacy and data security legislation should extend the FTC's jurisdiction to non-profits and common carriers, which often collect sensitive consumer information. Giving the FTC jurisdiction in these sectors would create a level playing field, ensuring that these entities would be subject to the same rules as others that collect similar types of data.

Regardless of any legislative changes, a significant increase in personnel would help the FTC ensure that American consumers' privacy is adequately protected. We currently have about 40 Full-Time Equivalents ("FTEs") devoted to privacy and data security issues—far fewer than

foreign data protection authorities. For example, the U.K. Information Commissioners' office has about 500 employees, and the Irish Data Protection Commissioner has about 110 employees. Although these entities have somewhat different mandates,[1] the contrast is stark. The FTC, as the federal entity primarily responsible for protecting consumers' privacy and data security in the United States (a much larger jurisdiction), should have more employees devoted to this effort.

You ask four specific questions about how the Commission would use additional resources, which I answer below.

1. **What resources would the FTC require to dramatically boost its enforcement activity with respect to privacy and data security? How would the FTC deploy new resources if it were to receive an additional $50 million for consumer protection and privacy? How about an additional $75 million? How about an additional $100 million? As part of your responses, please estimate the number of additional investigations and enforcement actions the FTC would likely be able to pursue.**

For the purposes of responding to this question, I assume that with $50 million in additional ongoing funding, we could hire approximately 160 more staff members; that with an additional $75 million annually, we could hire approximately 260 more staff; and that with an additional $100 million, we could hire approximately 360 more staff.[2] Assuming funding at these levels, I anticipate needing new management structures and support services to make the most effective use of these additional resources. Depending on the levels of additional funding and other considerations, below I have outlined one way in which we could allocate resources. We would, of course, consider any new privacy or data security legislation in determining how best to structure our work going forward.

Based on any of these three proposed levels of funding, we would consider adding at least three separate management units with the following responsibilities:

- **De novo enforcement:** One or more units would include some resources from our existing privacy division, which would be expanded to accomplish the following:
  - Devote additional staff to enforcement of the COPPA Rule;
  - Devote additional staff to financial privacy cases under the Gramm Leach Bliley ("GLB") Privacy and Safeguards Rules and the FCRA; and
  - Devote additional staff to Privacy Shield enforcement.

- **Order enforcement:** One or more units would include some resources from our existing enforcement division, and would expand the number of staff dedicated to conducting compliance reviews of our privacy and data security orders.

---

[1] For example, these entities enforce laws that protect consumers from government access to their data.

[2] Approximately two-thirds of our current budget is allocated to pay and benefits of staff, with about 16% allocated to overhead (such as rent and information technology) and the remaining 18% to other support expenses (such as expert witnesses, our consumer complaint database, and consumer and business education materials). Approximately 63% of our employees are attorneys or economists; the remainder are support staff such as investigators, technologists, and paralegals. In approximating the number of staff we could hire, we have assumed that any additional appropriation would be allocated similarly.

- **A new unit for policy, case generation, and targeting:** One or more units would be specifically devoted to conducting workshops, surveying legal developments in particular areas, writing advocacy comments and testimony, writing reports, and conducting 6(b) studies of industry. This unit would also include technologists to prepare original research on issues of interest, review referrals from privacy and security researchers, develop ideas for enforcement, and serve as a hub for technical expertise as needed on individual cases.

Each of these units would require new attorneys, paralegals, investigators, economists, administrative staff, electronic discovery staff, managers, and infrastructure (such as space). We would also plan to use some additional funds to pay outside experts in litigation and investigations, as privacy and data security investigations often involve complex facts and well-financed defendants.

You ask us to estimate the number of additional investigations and enforcement actions the FTC would likely be able to pursue. For reference, with our current allocation of about 40 staff devoted to privacy and security, we have brought on average about twenty privacy and data security cases per year over the past five years, and have investigated the privacy and security practices of many more companies. With more staff we would be able to bring more cases under our existing authority; providing us with additional authority would notably improve our ability to bring significantly more privacy and data security cases.

2. **If Congress were to direct the FTC to hire technologists to aid in case development, enforcement, rulemaking and/or policy recommendations, what resources would the FTC need to fulfill its consumer protection mission and how would the agency deploy those new resources? Specifically, describe the number of employees the agency would need, their roles and responsibilities, and how the FTC would use these resources to further its consumer protection mission.**

Currently, the Commission has about five full-time staff whose positions are classified as technologists. Beyond these specific full-time employees, the FTC has more than 40 investigators and lawyers who have developed technical expertise through their enforcement and policy work in the areas of big data, cybersecurity, the online advertising ecosystem, Internet of Things, artificial intelligence, and others. When the FTC needs more complex and richer information about a specific industry or technology, we supplement our internal technological proficiency by hiring outside technical experts to help us develop and litigate cases. We also keep abreast of technological developments in other ways, such as by hosting an annual event called PrivacyCon, in which we call on academics to present original research on privacy and security issues.

While we make the most of the technical resources we have, I believe we need to hire additional technologists to provide better support for our current enforcement and policy work. These technologists would serve the following roles:

- **Conducting original research:** Our existing Office of Technology Research and Investigation has conducted original research into, for example, data collection by children's apps, and the use of email authentication and anti-phishing technologies by

web-hosting services that market themselves to small businesses. With additional technologists, we would be able to conduct more studies of this nature.

- **Assisting in case targeting and development:** We currently have only around three technologist FTEs available to keep abreast of privacy and security research, work with attorneys to determine appropriate matters for investigation and enforcement, and to develop investigational plans to determine what evidence we might need to support a technology-related case. We could use more technologists to serve this function.
- **Serving on case teams:** The same three technologist FTEs noted above also review technical documents that we obtain in investigations and litigation; help attorneys conduct interviews, investigational hearings, and depositions of technical staff at companies; and provide technical advice to lawyers. Additional technologists would deepen and strengthen our litigation capabilities.
- **Pursuing technical tools for agency use in investigations:** Additional technologists could assist the Commission with acquiring or developing internal technical tools to analyze products and services for potential law violations.
- **Assisting with policy projects**: We could use additional technical expertise to support various technical policy projects. For example, last year we announced the results of our "IoT Home Inspector Challenge," in which we awarded prize money for a contest to create a way for consumers to be able to more easily update and patch Internet of Things' devices in their homes. A technologist assisted with that project, and additional technologists could assist with similar projects in the future. We could also use additional technologists to assist in drafting 6(b) orders for industry participants, and analyzing responses to those orders, to help us better understand specific industries and business practices.

To fulfil these roles, we anticipate needing 10-15 additional technologists. If the Commission were to receive significant new appropriations to boost its privacy and data security enforcement work, we would need to invest in even more technologists. Because current civil service rules for hiring can be time-consuming and inflexible in ways that might hinder our ability to attract and hire candidates with the most current and relevant experience, we are exploring how to classify these positions such that we could use direct authority for hiring.

3. **If the FTC received notice-and-comment rulemaking authority with respect to privacy and data security, would the FTC require additional resources to develop and update new rules without detracting from the agency's enforcement activity? If so, what resources would the FTC require?**

Yes. When Congress passed the Fair and Accurate Credit Transactions Act ("FACTA"), which amended the FCRA and resulted in the Commission creating more than ten separate Rules, the Commission spent more than 50,000 staff hours over the next three years on its implementation. This equates to eight full-time employees dedicated solely to that project for three years. We estimate that engaging in notice-and-comment rulemaking for comprehensive privacy or data security legislation would require at least the same, if not more, staff hours.

4. **What would the FTC be able to accomplish with 100 new attorneys focused on privacy and data security that it cannot do with current resources?**

The appropriation by Congress of money to bring in – and, importantly, continue to pay for – 100 new attorneys focused on privacy and data security would have a significant impact on the work of the Commission. With these additional resources, the FTC could devote more time not only to case generation and enforcement, but also to keeping abreast of new technologies and areas of privacy and data security concern through workshops, reports, and industry studies. The Commission would also be able to devote additional resources to compliance monitoring of companies under order for privacy and data security failures, and to engage in additional order enforcement litigation. Importantly, as described above, any influx of additional attorneys would also require additional appropriations for infrastructure, outside experts, and support staff such as technologists, paralegals, and investigators.

We appreciate your support of the Commission's efforts in the privacy and data security area. Should you need any additional information, please contact Jeanne Bumpus, Director of the FTC's Office of Congressional Relations, at (202) 326-2946.

Sincerely,

Joseph Simons
Chairman

JAMES L. MADARA, MD
EXECUTIVE VICE PRESIDENT, CEO

ama-assn.org
t (312) 464-5000

October 26, 2018

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission
400 7th Street, SW
Washington, DC 20024

Dear Chairman Simons:

On behalf of the physician and medical student members of the American Medical Association (AMA), I encourage the Federal Trade Commission to monitor insulin pricing and market competition and recommend enforcement action against manufacturers that engage in anticompetitive actions to the U.S. Department of Justice. Over the past several years, physicians have become increasingly concerned that the rapid rise in the price of insulin for patients is unrelated to the actual costs of research, development, commercialization, or production. Instead, physicians are concerned that anticompetitive factors may be present in the market for insulin. The consequences of an anticompetitive market could include worse health outcomes for patients due to artificially high and unaffordable prices of a critical medication that has been and should continue to be widely available and affordable.

Approximately six million Americans use insulin, a drug that has experienced dramatic price increases over the past decade. High insulin prices impact stakeholders throughout the health care system, but the consequences fall most heavily on patients. Insulin is one of the many essential drugs across all categories of pharmaceuticals to recently experience remarkable price increases. While a variety of complicated factors contribute to increases in insulin prices, we remain concerned that anticompetitive behavior by manufacturers and pharmaceutical benefit managers (PBMs) could be one of them.

To date, at least five states and a federal prosecutor are demanding information from insulin manufacturers and PBMs. In addition, class-action lawsuits have been brought on behalf of patients. For example, a class action complaint filed in Massachusetts in January 2017 points to evidence that, "[i]n 13 instances since 2009, Sanofi and Novo Nordisk raised the benchmark prices of their long-acting analog insulins, Lantus and Levemir, in tandem, 'taking the same price increase down to the decimal point within a few days of each other'...Eli Lilly and Novo Nordisk have engaged in the same lock-step behavior with respect to their rapid-acting analog insulins, Humalog and Novolog." The complaint further alleges that these pharmaceutical companies artificially inflated their list prices to secure positions on PBMs' formularies, with PBMs demanding higher rebates in exchange for including drugs on their preferred-drug lists. Similarly, three insulin manufacturers—Sanofi-Aventis, Novo Nordisk and Lilly—along with three of the largest PBMs—CVS Health, Express Scripts and OptumRx—are subject to a class action lawsuit, alleging that they together caused "rapid and lockstep price increases of more than 150 percent in insulin treatments." On the state level, in 2017, Nevada passed an act that requires the state's Department of Health and Human Services to compile a list of prescription drugs that it determines to be essential for treating diabetes. The manufacturers and PBMs associated with essential diabetes drugs will have to submit annual reports to the state containing drug cost information, which will be analyzed by the state and

reported on its website. However, pharmaceutical companies have begun challenging the Nevada law in court.

The implementation of the 21st Century Cures Act has been hampered by rapidly rising costs of prescription medication. The disease burden to patients, their families, and the health system imposed by diabetes is substantial. Access to affordable insulin is essential to ensuring patient health outcomes are not simply stabilized, but improved.

Should you have questions, please contact Shannon Curtis, Assistant Director of Federal Affairs, at shannon.curtis@ama-assn.org or 202-789-8510.

Sincerely,

James L. Madara, MD

100 CONSUMER BANKERS ASSOCIATION CENTENNIAL

CBA

HELPING FINANCE THE AMERICAN DREAM SINCE 1919.

May 8, 2019

The Honorable Frank Pallone
Chairman
Committee on Energy & Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Greg Walden
Ranking Member
Committee on Energy & Commerce
U.S. House of Representatives
2322 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Pallone and Ranking Member Walden:

On behalf of the Consumer Bankers Association (CBA), I thank the Energy & Commerce Committee for holding today's hearing, entitled "Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security." CBA is the voice of the retail banking industry whose products and services provide access to credit for consumers and small businesses. Our members operate in all 50 states, serve more than 150 million Americans, and collectively hold two-thirds of the country's total depository assets. As such, our members take seriously their responsibility to protect consumers' sensitive information and we would like to take the opportunity to share our views on a national data security and data privacy framework and the role of the Federal Trade Commission (FTC) in helping to protect consumers across the payment system.

The State of Data Privacy

In light of recent data breaches and abuses, consumers are rightly concerned about the manner in which their personal information is being collected and how this sensitive information is being both shared and protected. In 2018 alone, the number of data breaches in the U.S. totaled more than 1,200 according to the Identity Theft Resource Center. No industry was immune from breaches in 2018: business sector (46 percent), healthcare/medical industry (29 percent), banking/credit/financial industry (11 percent), government/military (8 percent), and the education sector (6 percent). However, it is important to note that the non-financial business sector, which is not subject to national data security requirements, was responsible for the overwhelming majority (93 percent) of the personal records compromised. In addition to breaches, there have been several noteworthy examples of misuse of customer data in the past year which warrant a review of industry practices and the scope of federal privacy laws and regulations, e.g. Cambridge Analytica gained access to private information on more than 50 million Facebook users.[1]

CBA members take seriously their responsibility to clearly explain the uses of consumers' data and to safeguard it against improper use and criminals attempting to steal it. Since the passage of the Gramm-Leach-Bliley Act (GLBA) in 1999, financial institutions have been required to provide their customers a clear privacy notice detailing information collection and sharing practices, which includes an opt-out for the sharing of information with non-affiliated third parties. This notice is provided at the beginning of the customer relationship and annually thereafter. GLBA and subsequent regulations also require banks to have in place data security protocols to safeguard sensitive consumer information and to report to federal authorities and affected consumers when a breach occurs. Banks are examined by their prudential regulators on these standards and if found to be non-compliant may face fines or other penalties.

[1] https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

1225 EYE STREET, NW, SUITE 550, WASHINGTON, D.C. 20005
consumerbankers.com

The low breach-rate of personally identifiable information (PII) at financial institutions compared to other sectors can be attributed to the common-sense safeguards required by GLBA and the industry's commitment to security. As a result, consumers trust financial institutions more than any other type of organization to keep their financial information secure, according to an August 2017 poll by Morning Consult.

Consumer Privacy

CBA supports consumers having reasonable control concerning the collection, use and sharing of personal data. However, we caution against national privacy legislation that may inhibit banks' ability to fulfill their contractual obligations to consumers. Compared to other industries, banks are subject to more stringent rules and lead in protecting consumers' PII and their privacy.

Pursuant to the GLBA, banks are required to protect the security and confidentiality of consumer records and information, and the law also requires banks to disclose their privacy practices and limits sharing PII with nonaffiliated third parties. Any Federal privacy law must consider the GLBA and other existing Federal privacy laws and preempt the growing patchwork of state laws that provide differing and inconsistent consumer protections. Otherwise, a consumer's privacy protections, including their ability to understand their rights, will depend on the state where the individual resides. While these state laws may be well-intentioned, they must be crafted to not hinder the free flow of data needed to provide consumers and businesses with financial products and services and process financial transactions.

As Congress considers the creation of a national data privacy framework, we must first recognize the differences in data collection among industries. Banks are required by federal law to collect certain information to conduct a customer transaction. For example, if a consumer wants to open a checking account, at a minimum pursuant to the Bank Secrecy Act, the bank must obtain certain information to fulfill its Customer Identification Program requirements, such as date of birth, address, and identification number. As an additional benefit to customers, banks also use personal data to develop banking products and services that are customized to a customer's needs. Utilizing consumer data to conduct financial transactions authorized by the consumer is far different than a social media platform collecting consumer data to sell to marketers.

It is also important that a federal privacy standard should not expand the scope of data that banks are responsible for protecting. GLBA requires banks to protect consumers "nonpublic personal information", which is defined, in part, as "[. . .] personally identifiable financial information, (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."[2] Consumer is defined to mean "an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personally, family, or household purposes, or that individual's legal representative."[3] An expansion of the definition of covered data or covered persons pursuant to a national standard would subject banks to unnecessary regulatory burden.

A national data protection and privacy law must also seek to promote innovation, investment and competition in the marketplace. The United States Constitution authorizes Congress to regulate interstate commerce, which includes the free flow of goods, services and consumer data. A patchwork of privacy laws at the state level will lead to higher costs for consumers and create barriers to innovation and investment. The assumption that preemption weakens existing state laws is a fallacy. In a world that is increasingly mobile, Americans and their devices constantly cross state borders.

[2] https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=15-USC-697127498-1137964384&term_occur=2&term_src=title:15:chapter:94:subchapter:I:section:6801

[3] https://www.law.cornell.edu/uscode/text/15/6809#4_A

Consumer protection should not depend upon which state you reside, but consumers should be covered by one unified, comprehensive federal standard.

From an international perspective, CBA also supports an open global economy that enables growth through the secure and efficient transfer of data across international borders. National data protection and privacy legislation should continue to support consumer privacy while also respecting and coordinating differences between U.S. and foreign privacy regimes.

National data protection and privacy legislation should be enforced by the FTC, unless a determination is made that it is appropriate for a different regulator to be the enforcement agency, e.g. prudential regulators for banks and credit unions. CBA is concerned that if state attorneys general are allowed to bring enforcement actions in federal court, there is a risk that each state will enforce the law differently. In addition, a national consumer privacy law should not provide for a private right of action.

Lastly, the California Consumer Privacy Act is the first major consumer privacy law to be adopted at the state level. This legislation was written hastily, and the state government is currently reviewing and revising portions of the law through both legislative and regulatory processes. As the California privacy law continues to evolve, it would be prudent for Congress to monitor issues with implementation and use their observations to draft a federal data privacy and security standard. Considering the importance of this issue and the impact it will have on both consumers and businesses, it is imperative that Congress is thoughtful in drafting meaningful legislation to protect consumers and provide businesses with certainty.

Data Security and Breach Notification

It is also critical that any conversation around data privacy also take seriously the security of data and the protocol for notifying customers in the event of a breach. Banks are on the front lines consistently monitoring for fraud and working to make consumers whole, no matter where a breach occurs. From operating advanced fraud monitoring systems to reissuing cards, CBA members spend considerable resources on preventing fraud. As a result, consumers rely on their financial institutions to communicate what to do in the event of a breach and to employ defenses to prevent fraud and identity theft.

Subsequent to Section 501(b) of GLBA, the financial regulators issued guidelines requiring banks to implement comprehensive, risk-based information security programs that include administrative, technical and physical safeguards to protect customer information. These safeguards are not static but flexible and scalable – applying to banks of all sizes. A similar framework should be applied to non-bank companies to ensure consumers' sensitive information is protected throughout the payment system.

Banks must also implement a risk-based response program in the event of a breach. The program includes an evaluation of the incident and an effort to prevent further unauthorized access as well as notice to the institution's primary federal regulator, appropriate law enforcement, and, importantly, the customers whose information was breached and could be misused. CBA supports legislation to require others in the payment system to provide timely notification to their customers in the event of a breach.

Today, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of a security breach of information involving PII.[4]

[4] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Twenty-four states currently have data security laws requiring a level of security procedures and practices to be in place to protect personal information.[5]

Congress has the constitutional authority to regulate interstate commerce through the Commerce Clause, which was written to prevent fragmentation of markets and to encourage the free flow of goods and services, including information, across the nation with minimal interference. Congress should take seriously its authority and enact a federal data security and breach notification standard and preempt the current patchwork of state laws. With the recent breaches that have put millions of consumers at risk, the need to pass legislation to establish such a standard could not be more evident. Protecting consumer information is a shared responsibility of all parties involved.

On behalf of our members, I would like to thank you for your consideration of our views. We look forward to working with the Committee to foster an environment that prioritizes the protection and privacy of consumer data while promoting consumer access to credit.

Sincerely,

Richard Hunt
President and CEO
Consumer Bankers Association

[5] http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx

May 8, 2019

Chair Jan Schakowsky
House Committee on Energy & Commerce
Rayburn House Office Building 2125
Washington, D.C. 20515

Ranking Member Cathy McMorris Rodgers
House Committee on Energy & Commerce
Rayburn House Office Building 2125
Washington, D.C. 20515

Dear Chair Schakowsky and Ranking Member McMorris Rodgers:

Internet Association[1] (IA) welcomes the opportunity to submit this letter for the record as part of the Committee's May 8 hearing: *"Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security."*

The internet industry appreciates the Committee holding this hearing to advance the conversation around an American approach to data privacy. Data is at the core of all modern U.S. businesses both online and offline, across every sector of the economy. For people to benefit from this transformation, there needs to be new rules of the road for everyone in the economy and society. This is why Internet Association and our members support federal privacy legislation to provide consumers meaningful control over and access to their personal information. The Federal Trade Commission (FTC) should continue to be the lead enforcement agency to ensure consistent application of federal law, and it should be provided the resources necessary to fulfil this mission.

The FTC does a commendable job enforcing privacy laws and advancing best practices to protect Americans' privacy. It has demonstrated a vigorous approach to privacy enforcement for two decades that achieves both immediate and long-term goals, by stopping inappropriate handling of consumer data, requiring companies to commit to plans designed to ensure data handling will be legally compliant in the future, and providing guidance on achieving regulatory compliance in areas where existing standards may be unclear.

Additional resources could enhance the FTC's ability to conduct meaningful enforcement of existing privacy laws and any future comprehensive federal data privacy regime that may include newly covered entities, data types, and regulatory obligations. Congress should also carefully consider any new authorities granted to the FTC as part of a larger privacy package.

In addition, the FTC has always embraced a mission of educating individuals on their rights and protections under the law, and this effort should be encouraged and appropriately resourced. The FTC also educates organizations on their obligations and best practices, such as the

[1] Internet Association represents https://internetassociation.org/our-members/.

recently launched Cybersecurity for Small Business campaign.[2] Such campaigns are incredibly valuable and should be appropriately resourced.

Internet Association and our member companies stand ready to work with this Committee and all other interested parties on an American approach to protecting people's privacy that allows for continued U.S. leadership in technology. The internet industry supports the passage of bipartisan privacy legislation this year.

Sincerely,

Michael Beckerman
President and CEO

[2] See more: https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

May 7, 2019

The Honorable Janice D. Schakowsky
Chairwoman
Subcommittee on Consumer Protection
& Commerce
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
Subcommittee on Consumer Protection
& Commerce
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

Re: Tomorrow's Hearing on "Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security"

Dear Chairwoman Schakowsky and Ranking Member McMorris Rodgers:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) in conjunction with tomorrow's hearing entitled "Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 116 million consumers with personal and small business financial service products. NAFCU and our members welcome the Committee taking an important step in holding this hearing to address consumer privacy and data security standards.

As NAFCU has previously communicated to the Committee, a major aspect of consumer privacy is ensuring the security of a consumer's financial data. While depository institutions have had a national standard on data security since the passage of the *Gramm-Leach-Bliley Act* (GLBA) over two decades ago, other entities who handle consumer financial data do not have such a national standard. We recognize that the Federal Trade Commission (FTC) plays an important role in overseeing data security outside of the regulated financial services sector. Still, their abilities are limited and more must be done. NAFCU believes that there is an urgent need for a national data security standard for entities that collect and store consumers' personal and financial information that are not already subject to the same stringent requirements as depository institutions under the GLBA.

We recognize that a legislative solution to establish such a standard is a complex issue, and thus NAFCU has established a set of guiding principles to help define key issues credit unions would like to see addressed in any comprehensive cyber and data security effort that may advance. These principles include:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to enact legislation to require entities to be accountable for costs of data breaches that result from negligence on their end.

- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under the GLBA, credit unions and other depository institutions are required to meet certain criteria for safekeeping consumers' personal information and are held accountable if those criteria are not met through examination and penalties. Unfortunately, there is no comprehensive regulatory structure akin to the GLBA that

covers other entities who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on depository institutions under the GLBA.

- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant but would provide an important benefit to the public at large.

- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised personally identifiable information when associated accounts are involved.

- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.

- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by those who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.

- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the negligent entity who incurred the breach.

NAFCU looks forward to working with the Committee to address concerns with consumer privacy as it relates to the broader topic of data security. We are also pleased to work with those in industry to try to find common ground on a comprehensive proposal. We would urge the Committee to work collaboratively with the Financial Services Committee to advance comprehensive data security legislation in the year ahead. In the meantime, we also encourage the Committee to urge the FTC to use its authority to hold those responsible for data breaches that harm consumers accountable.

On behalf of our nation's credit unions and their more than 116 million members, we thank you for your attention to this important matter. Should you have any questions or require any additional information please contact me or Janelle Relfe, NAFCU's Associate Director of Legislative Affairs, at 703-842-2838 or jrelfe@nafcu.org.

Sin[redacted]

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Subcommittee on Consumer Protection & Commerce

May 8, 2019

The Honorable Janice D. Schakowsky
Chairman
U.S. House of Representatives
Committee on Energy and Commerce
Consumer Protection and Commerce Subcommittee
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
U.S. House of Representatives
Committee on Energy and Commerce
Consumer Protection and Commerce Subcommittee
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Schakowsky and Ranking Member McMorris Rodgers:

The Confidentiality Coalition appreciates the opportunity to submit this letter to the U.S. House of Representatives Consumer Protection and Commerce Subcommittee hearing, "Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security."

We are a broad group of organizations—hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, clinical laboratories, patient groups, home care providers, and others—working to ensure that we as a nation find the right balance between the protection of confidential health information and the efficient and interoperable systems needed to provide high quality care.

The Health Insurance Portability and Accountability Act (HIPAA) established acceptable uses and disclosures of individually-identifiable health information within healthcare delivery and payment systems for the privacy and security of health information. The Confidentiality Coalition believes that to the extent not already provided under HIPAA, privacy rules should be consistent so that persons and organizations not covered by HIPAA that create, compile, store, transmit, or use health information operate under a similar expectation of acceptable uses and disclosures.

The Confidentiality Coalition has long supported the Federal Trade Commission's (FTC) oversight of personal health records (PHR) that reside in non-HIPAA covered entities, which was provided in the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub L. No. 111-5 §

13407). As required by HITECH, the FTC promulgated rules to carry out this authority. In 2010, the FTC finalized a Health Breach Notification Rule that requires vendors of PHRs, PHR-related entities, and third-party service providers for a vendor of PHRs to notify the FTC in the event of a breach. As the committee continues to explore the government's role in strengthening protections for Americans' privacy and data security, the coalition supports a federal data privacy framework that is consistent nationally and includes similar expectations to that of HIPAA for acceptable uses and disclosures for non-HIPAA covered health information. This is vital to maintain consumer trust in the healthcare system.

Thank you for examining this important issue and please feel free to reach out to Tina Olson Grande, Senior Vice President for Policy at the Healthcare Leadership Council on behalf of the Confidentiality Coalition, at (202) 449-3433 or tgrande@hlc.org with any questions. Enclosed you will find the Confidentiality Coalition's Principles on Privacy and a list of coalition members.

Sincerely,

Tina Olson Grande
Healthcare Leadership Council on behalf of the Confidentiality Coalition

Enclosure

MEMBERSHIP

AdventHealth
Aetna, a CVS Health business
America's Health Insurance Plans
American Hospital Association
American Society for Radiation Oncology
AmerisourceBergen
Amgen
AMN Healthcare
Anthem
Ascension
Association of American Medical Colleges
Association of Clinical Research Organizations
athenahealth
Augmedix
Bio-Reference Laboratories
Blue Cross Blue Shield Association
BlueCross BlueShield of North Carolina
BlueCross BlueShield of Tennessee
Cardinal Health
Cerner
Change Healthcare
Children's Hospital of Philadelphia (CHOP)
CHIME
Cigna
Ciox Health
City of Hope
Cleveland Clinic
College of American Pathologists
Comfort Keepers
ConnectiveRx
Cotiviti
CVS Health
Datavant
dEpid/dt Consulting Inc.
Electronic Healthcare Network Accreditation Commission
EMD Serono
Express Scripts
Fairview Health Services
Federation of American Hospitals
Genetic Alliance
Genosity
Healthcare Leadership Council
Hearst Health
HITRUST
Intermountain Healthcare
IQVIA
Johnson & Johnson
Kaiser Permanente
Leidos
Mallinckrodt Pharmaceuticals
Marshfield Clinic Health System
Maxim Healthcare Services
Mayo Clinic
McKesson Corporation
Medical Group Management Association
Medidata Solutions
Medtronic
MemorialCare Health System
Merck
MetLife
National Association for Behavioral Healthcare
National Association of Chain Drug Stores
National Community Pharmacists Association
NewYork-Presbyterian Hospital
NorthShore University Health System
Pfizer
Pharmaceutical Care Management Association
Premier healthcare alliance
SCAN Health Plan
Senior Helpers
State Farm
Stryker
Surescripts
Teladoc
Texas Health Resources
Tivity Health
UCB
UnitedHealth Group
Vizient
Workgroup for Electronic Data Interchange
ZS Associates

Revised May 2019

PRINCIPLES ON PRIVACY

1. All care providers have a responsibility to take necessary steps to maintain the confidentiality and trust of patients as we strive to improve healthcare quality.

2. The framework established by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule should be maintained. HIPAA established a uniform framework for acceptable uses and disclosures of individually-identifiable health information within healthcare delivery and payment systems for the privacy and security of health information to enable the provision of health care services to patients. HIPAA follows the widely accepted Fair Information Practices standards (FIPS.)

    a. The HIPAA Privacy Rule, through "implied consent," permits the sharing of medical information for specified identified healthcare priorities which include treatment, payment and healthcare operations (as expected by patients seeking medical care.) This model has served patients well by ensuring quick and appropriate access to medical care, especially in emergency situations where the patient may be unable to give written consent.

    b. The HIPAA Privacy Rule requires that healthcare providers and health plans limit disclosure of protected health information to the minimum necessary to pay for healthcare claims and other essential healthcare operations. This practice provides privacy protection while allowing for continued operations. Minimum necessary is relatively easy and simple to administer and practice.

3. Personal health information must be secured and protected from misuses and inappropriate disclosures under applicable laws and regulations.

4. Providers should have as complete a patient's record as necessary to provide care. Having access to a complete and timely medical record allows providers to remain confident that they are well-informed in the clinical decision-making process.

5. Privacy frameworks should be consistent nationally and across sectors so that providers, health plans, and researchers working across state lines and with entities governed by other privacy frameworks may exchange information efficiently and effectively in order to provide treatment, extend coverage, and advance medical knowledge, whether through a national health information network or another means of health information exchange.

6. The timely and accurate flow of de-identified data is crucial to achieving the quality-improving benefits of national health information exchange while protecting individuals' privacy. Federal privacy policy should be consistent with the HIPAA regulations for the de-identification and/or aggregation of data to allow access to properly de-identified information. This allows researchers, public health officials, and others to assess quality of care, investigate threats to the public's health, respond quickly in emergency situations, and collect information vital to improving healthcare safety and quality.

7. For the last 20 years, the HIPAA privacy standards have engendered consumer trust. Any future legislation or rulemaking that addresses identifiable health information should conform with consumers' expectations.

Revised January 2019

Additional Questions for the Record

Subcommittee on Consumer Protection and Commerce
Hearing on
"Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security"
May 8, 2019

The Honorable Joseph J. Simons, Chairman
The Federal Trade Commission

The Honorable Jan Schakowsky (D-IL)

1. **Expert witnesses play an integral role in the Federal Trade Commission's (FTC) enforcement of both competition and consumer protection laws, particularly in complex mergers or technical matters concerning privacy and data security. The FTC's FY2020 Budget Justification states that the Commission faces significant resource challenges due to the rising costs of expert witnesses' contracts.**

    a. **On average, how much does the FTC spend on expert witnesses in an individual case?**

    b. **How much does the FTC spend on expert witnesses per year?**

    c. **By how much have the costs of expert witnesses increased during the past 10 years?**

    d. **Has the FTC ever chosen not to pursue an enforcement action due to the prohibitive costs of expert witnesses?**

Thank you for your attention to this important issue. There are some complexities associated with our expert witness engagements, which we would like to clarify for the Subcommittee. We caution that reliance on average numbers over time may present a somewhat inaccurate view of the facts on the ground, given that our enforcement work may result in wide year-to-year variances in spending. Given some significant differences between competition and consumer protection cases, this response breaks out information separately for each of our two enforcement missions.

Competition Cases

When a competition case goes to litigation (versus settlement or closing), expert witness costs typically increase exponentially for that matter. As a result, the agency's annual expert witness costs for competition matters in a given fiscal year are largely a function of the number and types of competition cases the Commission must litigate during the course of that year. Since each additional litigated case may lead to millions of dollars in additional expert fees, even very small changes in the total number of competition cases per year can have a dramatic impact on the

agency's overall spending on expert fees. Although most of our cases ultimately settle, the total number of litigated cases can vary widely year to year.

Unfortunately, the agency has a limited ability to control this primary driver of our expert costs. This is particularly true with respect to merger matters, where outside parties dictate the volume, nature, and timing of their deals. The Commission votes out a complaint when it has reason to believe that a competition enforcement action is in the public interest. Post-vote, the course of litigation (and possible settlement) is determined in large part by the defendants and, of course, the judge or judges. Among other factors, defendants may choose to retain one or more experts of their own, which can affect our expert strategy.

In general, we have observed that the kinds of experts qualified for this kind of work are becoming more expensive. In an increasingly data-rich world, each case requires more of an expert's time, and more support resources to process data and increasingly large volumes of documents. Our expert budget is depleted not only by higher prices per hour worked, but also by the need for experts to spend more time preparing for each case, and the need for more support resources to manage each case.

On the competition side, we have determined that the range of total expert costs for cases that are fully litigated (meaning a preliminary injunction, administrative hearing on the merits or both) in the last five years is $583,100 - $6.90 million.

The remaining, requested data points for our competition cases are as follows:

Fiscal Year	Expert Spending*
2008	$3.05 million
2009	$3.40 million
2010	$3.16 million
2011	$2.97 million
2012	$2.09 million
2013	$2.98 million
2014	$4.84 million
2015	$10.03 million
2016	$12.21 million
2017	$11.46 million
2018	$15.80 million
**Some years' expenditures may change due to ongoing work*	

To date, the Commission has managed allocated funds to pay the expert witness fees needed to pursue vigorous competition enforcement on behalf of consumers. We are, however, increasingly concerned about our ability to continue to do so.

Consumer Protection Cases

Average expert cost per case: Between FY16 and FY18, the Commission filed an average of 71 consumer protection cases (mostly in federal court) per year, spending approximately $30,000 per case on expert witness contracts. The Commission uses experts in approximately 44 consumer protection matters per year, spending an average of approximately $49,000 on expert witness contracts in each of those cases.

Total yearly expert costs: Between FY16 and FY18, the Commission spent approximately $2.16 million on expert witness contracts for consumer protection cases per year, and is on track to obligate $2.28 million during FY19.

Expert spending over past 10 years: The Commission's expert spending on consumer protection cases has remained steady over the past 10 years. In FY 2008, the Commission expended approximately $2.07 million on expert contracts in consumer protection cases, and is on track to obligate $2.28 million during FY19.

2. **Since announcing the Hearing on Competition and Consumer Protection in the 21st Century, the FTC has held 13 hearings examining topics ranging from the FTC's vertical merger policies to privacy and data security. Some critics have observed that many of the panelists at these hearings, particularly economists, have significant financial ties to large corporations that are regulated by FTC, including Facebook, Google, and Amazon. One report suggests that more than a third of the scholars participating in the FTC's hearings have financial ties to Google. I am concerned by these criticisms because it suggests that the FTC is not hearing from unbiased points of view at these hearings.**

    a. **Does the FTC require panelists before appearing as an expert at FTC hearings or workshops to disclose financial ties to industry? If so, what are those requirements?**

    b. **How many panelists at the FTC's Hearings on Competition and Consumer Protection in the 21st Century disclosed financial ties to entities within the FTC's jurisdiction?**

    c. **Did the FTC publicize any such financial ties before the hearings, and, if not, why not?**

The FTC has taken significant steps to feature a wide variety of perspectives during the hearings. We have invited legal and economic academics, legal and economic consultants, public interest groups, public advocacy groups, and representatives of businesses and industries to our hearing sessions. By the time the hearings conclude on June 12, we will have hosted 393 unique non-FTC participants for 23 days of public hearings.

During hearings and workshops, the FTC generally asked panelists the following two questions:

1. Whether any third party funded or otherwise provided financial assistance for the research/analysis/commentary you will present at the hearing? If yes, who?

2. Whether any third party will compensate you for your participation at the hearing or otherwise provide financial assistance for your participation (e.g., reimburse your travel expenses)? If yes, who?

If a panelist answers yes to either question, we include that information and the name of the third party within the bios that we publish for each hearing. In addition, if a panelist is currently working for a corporation, we include that information in their bio as well. Bios and information are available on our website.

We have sought public input and, to the greatest extent possible, facilitated informed comments from a wide range of interested parties. For example, before each hearing, we have released an agenda, list of participants, and a list of specific questions designed to solicit comments. The public comment period has been open before each hearing, allowing commenters to raise issues for discussion at the public session. The comment period has also extended well beyond the date of each specific hearing, to allow interested parties to comment on the discussion at the public session. We stream each hearing session live, and place a video of the hearing session on our website for those who could not attend or watch live. We also release a transcript of each hearing shortly after conclusion of a session. We have, to date, received close to 900 unique comments on our hearings topics. The FTC posts all germane comments online shortly after we receive them, allowing the public to comment on points raised in the public comments. The public comments will receive the same review, scrutiny, and consideration as the comments and discussion at our hearings. There are no restrictions on who can comment, and I believe the public written comments are as important and valuable as the commentary at our hearing sessions. We have also consulted the substantial body of academic literature available on each topic we have taken testimony on, in preparation for each hearing.

The Commission and its staff regularly review arguments and advocacy of parties, persons, and interest groups who appear before us on enforcement and policy matters. Often, they do not disclose their source of funding, their direct or indirect interest in the matter they bring before us, or how they (or their clients or funders) might benefit from the outcome they seek. In those situations, we carefully evaluate the information and arguments on the merits. We will do the same here.

3. **The FTC's Bureau of Economics plays an important role in both the FTC's competition and consumer protection enforcement. But reports indicate that the Bureau of Economics approaches privacy and data security cases with skepticism, based on a view that few privacy or data security practices cause injury, or that consumers do not meaningfully engage with privacy policies (and therefore cannot be deceived by them).**

    a. **How does the Bureau of Economics participate in the FTC's privacy and data security matters? To what extent does the Bureau of Economics influence whether a privacy or data security investigation continues?**

    b. **Has the Bureau of Economics dissented from or otherwise opposed any of the FTC's privacy enforcement matters in the past 5 years and, if so, how many?**

The Bureau of Economics supports the FTC's privacy and data security work by providing high quality, up-to-date economic analysis and advice. The Bureau of Economics provides the Commission with independent economic analysis of the harms and potential harms stemming from alleged Section 5 violations. The Bureau of Economics continues to develop innovative solutions to deal with the known difficulties of measuring the harm associated with privacy and data security practices.

The Bureau of Economics reviews every complaint or settlement recommendation that the Bureau of Consumer Protection makes on privacy and data security matters, as they do in all enforcement matters. The Bureaus discuss these matters at the staff and management level. In some instances, the Bureau of Economics may persuade the Bureau of Consumer Protection to modify, add, or drop certain complaint allegations or theories of liability. The Bureau of Consumer Protection then presents its final recommendation to the Commission, and the Bureau of Economics provides a separate recommendation memorandum to the Commission.

In the past five years, the Bureau of Economics has disagreed with three of the Bureau of Consumer Protection's privacy and data security case recommendations (out of approximately 60 total recommendations). In a few other cases, the Bureau of Economics has supported BCP's recommended action, but raised issues about particular proposed complaint allegations.

4. **On June 11, 2019, the FTC will hold a workshop on online event tickets. I have heard reports of a number of consumer protection issues concerning online event tickets that raise serious concerns and I hope the FTC will consider addressing these issues during its workshop. For example, I have heard concerns that primary ticket platforms have begun forcing purchasers to disclose personally identifiable information by creating an account with the primary ticket seller to use a ticket, even when tickets are resold on a secondary market. I have also heard complaints about primary ticket sellers that hold tickets back from the market pursuant to agreements with venues, artists, or other partners. In addition, I have received complaints about primary ticket vendors putting technological restrictions on the transfer of tickets, which can prevent ticket holders from reselling or giving away tickets if they cannot attend the event.**

    a. **Will the FTC examine these issues at its upcoming hearing on online event tickets?**

Yes, the June 11 Online Event Ticketing Workshop will examine the issues that you raise and their possible impact on consumers in the online event tickets marketplace.

    b. **Has the FTC received similar complaints from consumers?**

The most common consumer complaints we receive about online event ticketing concern either hidden or inadequately disclosed ticketing fees in the primary and secondary markets, or reports that ticket resellers misled consumers to believe they were purchasing tickets from the venue or authorized seller at face value (when in fact they were purchasing tickets from resellers at a significant markup). The Commission has also received several thousands of consumer comments in connection with the upcoming ticketing workshop. Those comments

overwhelmingly concern hidden or inadequately disclosed ticketing fees and/or the high cost of such fees. While the FTC may also have received consumer complaints or comments regarding the practices you outline, they do not appear to be as prevalent.

c. Do you agree that, if true, these practices raise concerns about unfair or deceptive practices in the market for online event tickets?

These practices may raise questions about transparency and consumer understanding in the online event tickets marketplace; however, it is unclear whether requiring ticket buyers to provide personally identifying information, holding back tickets for later sale, or restricting the transfer of tickets would be unfair or deceptive acts or practices under Section 5 of the FTC Act.

The Honorable Bobby L. Rush (D-IL)

1. **In 2014, the Federal Trade Commission (FTC) published a report called "Data Brokers: A Call for Transparency and Accountability" that shed light on the secretive world of data brokers that buy and sell vast amounts of consumer personal information, often entirely behind the scenes. The FTC's report called on Congress to pass legislation that would require data brokers to be more transparent and give consumers the right to opt-out, among other things.**

   a. **Do you still agree that Congress should pass legislation addressing data brokers?**

The current Commission has not taken a position on data broker legislation. I support federal privacy and data security legislation that would give the Commission authority to seek civil penalties for first-time privacy and data security violations; conduct targeted APA rulemaking; and exercise jurisdiction over common carriers and non-profit entities.

2. **While innovation in the tech industry is having a tremendous impact on our economy and the lives of everyday Americans, it is also creating new challenges in protecting consumers and competitive markets. I have heard reports of certain online platforms giving their subsidiary businesses preferential treatment over their competitors.**

   a. **Are you looking into anti-consumer and anti-competitive behaviors of this nature?**

   b. **In your opinion, does the FTC currently have the authority and capacity to curtail this behavior?**

As more and more of the nation's commerce takes place on online platforms, the operation of these platforms has received increased scrutiny by both the public and the antitrust agencies. I believe the FTC has many of the tools it needs to protect consumers online, although I have called for Congress to give the FTC the authority to seek civil penalties for initial privacy violations, which would create an important deterrent effect. Moreover, I believe consumers

would benefit if the FTC had broader enforcement authority to take action against common carriers and non-profits, which it cannot currently do under the FTC Act. That said, the FTC is vigilant in its oversight of the internet economy, and we will not hesitate to take strong and appropriate action against any act or practice that violates any statute we enforce.

The Bureau of Competition recently announced the creation of a Technology Task Force ("TTF") that will enhance the Commission's antitrust focus on technology-related ecosystems, including technology platforms as well as markets for online advertising, social networking, mobile operating systems, and apps. The TTF will monitor competition in U.S. technology markets, investigate any conduct in these markets that may harm competition, and, when warranted, take actions to ensure that consumers benefit from free and fair competition.

The FTC does not publicly comment on pending law enforcement investigations. However, I can provide some guidance as to the applicable legal standards under current law.

As a threshold matter, it is important to appreciate that there are no special antitrust rules for online platforms. The same core antitrust laws and principles that apply generally across the economy apply to online platforms as well. This includes the laws relating to monopolization. Whether a firm is an online platform or a company that operates brick-and-mortar stores, if the firm has monopoly power or a dangerous probability of acquiring such power, the firm is subject to the same prohibitions under the U.S. antitrust laws: it cannot engage in anticompetitive conduct that tends to contribute to the acquisition or maintenance of monopoly power and lacks a procompetitive efficiency justification.

If FTC staff were to analyze an allegation that an online platform had violated the antitrust laws by discriminating against competitors, FTC would apply the test described above. To evaluate whether an online platform might have monopoly power, we would consider the online platform's share of the relevant market (or markets) in which it competes, as well as other factors (such as the existence and magnitude of barriers to entry). If a platform with monopoly power were to extend some form of preferential treatment to its own business units in a way that was alleged to contribute to the improper acquisition or maintenance of monopoly power, that conduct would be analyzed through a careful and fact-specific inquiry that considered the nature of the conduct, the extent to which it excluded competition, and any efficiency justifications.

As with most antitrust analysis, the conduct you describe would be neither automatically legal or automatically illegal; the specific nature of the conduct, and its positive and negative effects on competition and consumers, would matter very much. The U.S. antitrust laws do not impose a universal duty to deal with one's competitors on the same terms as with other divisions of one's own company. The antitrust laws do, however, recognize that certain forms of adverse treatment of competitors can, under appropriate circumstances, give rise to antitrust liability when the conduct contributes to the wrongful acquisition or maintenance of monopoly, and thereby harms competition. The FTC's talented and hard-working staff invest considerable time and energy to identify conduct that unlawfully harms competition and consumers in all areas of the economy, including online platforms, and will continue to do so.

3. **As all of you know, robocalls are extremely burdensome on consumers and every effort needs to be taken to ensure that consumers are not being taken advantage of by these unscrupulous actors. I am also concerned by the reports I have heard that robocalls are now being used by online contact lens retailers to usurp the verification of contact lens prescriptions, placing consumers at an even greater risk of receiving the wrong Class II or III medical devices.**

    a. **Do you agree that efforts need to be taken to update the passive verification process?**

When Congress enacted the Fairness to Contact Lens Consumers Act ("FCLCA"), it determined that passive verification was necessary to balance the interests of prescription portability and consumer health. Congress was aware that, in some instances, passive verification could allow sellers to sell contact lenses based on an invalid or inaccurate prescription, and that this could potentially lead to health risks. In the May 28, 2019 Supplemental Notice of Proposed Rulemaking ("SNPRM"), the Commission proposed several changes to improve the passive verification process. The Commission proposed that sellers who use automated telephone verification messages would have to: (1) record the entire call and preserve the complete recording; (2) begin the call by identifying it as a prescription verification request made in accordance with the Contact Lens Rule; (3) deliver the verification message in a slow and deliberate manner and at a reasonably understandable volume; and (4) make the message repeatable at the prescriber's option. This proposal would enable prescribers to better fulfill their role as protectors of patients' eye health because prescribers cannot correct and police invalid, inaccurate, and expired prescriptions if they cannot comprehend a seller's verification request.

Additionally, the Commission proposed changes that would increase patients' access to their prescriptions, maintain patient choice and flexibility, and potentially reduce the number of verification requests. Under the proposal, a prescriber, with the patient's verifiable affirmative consent, has the option to provide the patient with a digital copy of the prescription in lieu of a paper copy. Moreover, although the Rule has always required that prescribers, upon request, provide any person designated to act on behalf of the patient with a copy of the patient's valid contact lens prescription, the Rule did not prescribe a time limit within which this copy had to be provided. The Commission proposed requiring that a prescriber respond to requests for an additional copy of a prescription within forty business hours. To facilitate patients' ability to use their prescriptions, another proposed change would require sellers to provide a mechanism that would allow patients to present their prescriptions directly to sellers.

Finally, the Commission proposed amending the prohibition on seller alteration of prescriptions to address concerns about the misuse of passive verification to substitute a different brand and manufacturer of lenses. The proposal requires a seller who makes an alteration to provide a verification request to the prescriber that includes the name of a manufacturer or brand other than that specified by the patient's prescriber. There is a proposed exception if the patient entered that manufacturer or brand on the seller's order form or the patient orally requested it from the seller.

The Commission will consider comments received in response to the SNPRM and, if appropriate, make changes before issuing a final rule.

b. Do you agree that robocalls need to be eliminated from use within the passive verification system?

No, I do not agree with categorically eliminating the role of automated technology within the passive verification system. An effective verification process enables prescribers, when necessary, to prevent improper sales and allows sellers to provide consumers with their prescribed contact lenses without delay. The FCLCA expressly permits telephone communication for verification. It would be contrary to Congressional intent to prohibit the use of automated technology for the purpose of prescription verification. The Commission does not have empirical data showing the frequency of incomplete or incomprehensible automated telephone messages, or supporting a claim that a phone call with an automated message is necessarily less reliable than one with a live person. Rather, the evidence suggests that these calls can be an efficient method of verification. The Commission recognizes, however, the burden on prescribers and potential health risk to patients from incomplete or incomprehensible automated telephone messages. As described in response to question 3.a, the Commission has proposed changes to automated telephone messages that would improve the verification process.

c. Could you support updating the Fairness to Contact Lens Consumers Act to eliminate robocalls and update the passive verification system to include secured emails and patient portals to verify and document contact lens prescription verification?

I would not support categorically eliminating the role of automated phone call technology within the passive verification system. I do support clarifying that emails and portals would be acceptable mechanisms for prescription verification. Under the current Rule, a "seller may sell contact lenses only in accordance with a contact lens prescription for the patient that is: (1) Presented to the seller by the patient or prescriber directly or by facsimile; or (2) Verified by direct communication." 16 C.F.R. § 315.5(a). Because the Rule's definition of direct communication already includes electronic mail, a seller and a prescriber currently could use email during the verification process. In the December 7, 2016 Notice of Proposed Rulemaking ("NPRM"), the Commission made an initial determination that a portal could be used by a prescriber or a patient to "directly" present a contact lens prescription to a seller. The Commission will consider comments received in response to this initial determination and, if appropriate, make changes before issuing a final rule.

4. In December 2016, the FTC issued a Notice of Proposed Rulemaking to update the Contact Lens Rule. As a part of this process, providers and manufacturers of contact lenses urged the FTC to require common-sense changes to the current contact lens market, including quantity limits and ways to update methods of communication under the passive verification process. The FTC responded by stating that there was insufficient evidence that consumers are buying excessive quantities of contact lenses and that it did not have the statutory authority to update the passive verification process.

a. **Do you support efforts to ensure patient safety regarding the current proposed rulemaking process that will include patients only receiving contact lenses as prescribed under the valid prescription?**

The Commission does not believe patients should be able to purchase contacts without a valid prescription. The SNPRM's proposed changes improve patient access to contact lens prescriptions and address concerns with the passive verification requests and alterations by sellers.

5. **Last May, Rep. Michael Burgess (R-TX) and I led a letter to the FTC that laid out several concerns we have regarding the FTC rulemaking process around the Fairness to Contact Lens Consumers Act. In total, over 50 members of Congress signed this letter where we discussed the lack of enforcement action by the FTC to address the illegal sales of contact lenses and the burdensome new requirements on eye care providers.**

   a. **Has the FTC investigated or independently audited any online sellers to determine the number of lenses provided to patients?**

The Commission has not audited online sellers to determine the number of lenses provided to patients.

   b. **What enforcement mechanisms has the FTC used to ensure that sellers are not enabling the circumvention of state laws governing prescription renewal or harming patients by providing excessive numbers of contact lenses?**

In the NPRM, the Commission considered the issue of patients purchasing excessive quantities of contact lenses. Although concerned with anecdotal reports, the Commission concluded that the evidence did not show that the sale of excessive amounts of contact lenses is a widespread problem.[1] Furthermore, a prescriber who receives a verification request for an excessive amount of lenses can contact the seller to prevent the sale from being completed. Staff has investigated specific complaints of illegal sales related to excessive quantities. We will continue to monitor the marketplace, taking action against violations as appropriate.

   c. **How often has the FTC acted on this important safety issue?**

As discussed in the response to question 5.b, the Commission does not believe that the evidence shows that excessive sale of contact lenses is a widespread problem. The Commission does, of course, recognize the importance of patient safety. Staff will continue to monitor the marketplace and, if appropriate, take action.

6. **Many businesses are increasingly dependent on digital platforms that they do not own or operate to connect with customers.**

---

[1] NPRM at 88549-50; *see also* Vision Council, U.S. Optical Market Eyewear Overview 13 (2018), https://www.ftc.gov/sites/default/files/filefield_paths/steve_kodey_ppt_presentation.pdf (noting that 82% of contact lens users had an eye exam within the last 12 months and over 95% had an exam within the last two years).

a. **With current statutory authorities in mind, what can be done to protect consumers if companies that operate these platforms offer subsidiary business products and restrict or disadvantage competitors with similar businesses on these platforms? What is the FTC doing to curtail it?**

b. **One example of how a platform operator might harm consumers is by prohibiting businesses from communicating with their customers through that platform. Do you believe that this sort of behavior must be addressed and, if so, does the FTC currently have the statutory authority to do so?**

Please see the answer to question 2.

7. **It has been brought to my attention that the leading internet browser has been considering a major change in what type of information is available to consumers in their product, reducing the available information that consumers use to defend themselves against a host of online threats like phishing and content spoofing.**

    a. **As the agency charged with protecting our nation's consumers and enforcing our data privacy laws, do you have concerns about what this practice means for consumers and their data privacy and security?**

    b. **Have you discussed this issue with the browsers or asked them to explain their changes and how they will impact consumer safety online? If not, do you intend to?**

I understand your question to refer to how browsers display certain digital certificates in their user interface. When properly validated, digital certificates serve as proof that consumers are communicating with an authentic website and not an imposter. They also serve to encrypt traffic between a consumer's browser and a site's web server.

In May 2018, Google announced that it would change its user interface in its Chrome browser to remove certain indicators of the presence of an expensive digital certificate – called an extended validation certificate – such as green text and a padlock icon. I have not discussed these changes with Google. Consumers' secure online experiences depend on many factors, and the ecosystem continues to evolve quickly. I do not believe that the Commission should promote one type of certificate over another, or prescribe how certificates should be displayed in user interfaces.

The Commission is committed to promoting consumer safety online. In addition to our enforcement work, detailed in the Commission's written testimony, we engage in extensive consumer education, examples of which you may find here: https://www.consumer.ftc.gov/articles/0009-computer-security.

The Honorable Cathy McMorris Rodgers (R-WA)

1. **Chairman Simons, the FTC has existing rulemaking authority but is now asking Congress for additional APA rulemaking authority. Please answer the following questions about the Commission's existing rulemaking authority:**

    a. **When was the most recent opened rulemaking proceeding initiated? Please include the statutory authority permitting or directing the rulemaking.**

    b. **When was the most recent completed rulemaking proceeding completed? Please includes the statutory authority permitting or directing the rulemaking.**

The FTC opened its most recent proceeding to promulgate a new substantive rule in November 2018.[2] The 2018 Economic Growth, Regulatory Relief, and Consumer Protection Act, among other things, required that nationwide consumer reporting agencies provide free electronic credit monitoring services to active duty military consumers. It also required the FTC to issue regulations clarifying the meaning of certain terms used in the Act, as well as clarifying what constitutes appropriate proof that an individual is an active duty military consumer.[3]

In addition, the FTC reviews all of its existing rules periodically to seek information about their costs and benefits and their regulatory and economic impact. Most recently, in March 2019 the FTC announced a regulatory review of, and invited public comment on, the Franchise Rule.[4] The Franchise Rule makes it an unfair or deceptive act or practice for franchisors to fail to give prospective franchisees a Franchise Disclosure Document providing specified information about the franchisor, the franchise business, and the terms of the franchise agreement; it also prohibits related misrepresentations by franchise sellers. The Commission issued the original Franchise Rule in 1978 pursuant to its authority under Section 5 of the Federal Trade Commission Act to proscribe unfair or deceptive acts or practices.

In terms of completed new rules (as opposed to amendments of existing rules), the most recent new substantive rule issued by the Commission was the Business Opportunity Rule.[5] The Business Opportunity Rule governs disclosure requirements and prohibitions for business opportunities. The legal basis for the rule is Section 18 of the FTC Act, 15 U.S.C. § 57a, which authorizes the Commission to promulgate, modify, and repeal trade regulation rules that define with specificity acts or practices in or affecting commerce that are unfair or deceptive within the meaning of Section 5 of the FTC Act.

In the first half of 2019, the FTC completed its regulatory review for a number of rules and closed out those rulemaking proceedings. For example, the FTC amended its trade regulation rule concerning the labeling and advertising of home insulation to clarify, streamline, and

---

[2] *See* 83 Fed. Reg. 57693 (Nov. 16, 2018).
[3] *See* Pub. L. No. 115-174, § 302(d).
[4] *See* 84 Fed. Reg. 9051 (Mar. 13, 2019).
[5] *See* 72 Fed. Reg. 76815 (Dec. 8, 2011).

improve existing requirements; retained without modification the trade regulation rule concerning preservation of consumers' claims and defenses; and retained without modification its rule implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM").[6] Both of the trade regulation rules were issued under Section 18 of the Federal Trade Commission Act, 15 U.S.C. § 57a. The CAN-SPAM rule was issued under 15 U.S.C. §§ 7701-7713, which provides for both mandatory rulemaking and discretionary regulations concerning certain statutory definitions and provisions.

2. **Chairman Simons, currently, does the Commission utilize an expert witness for data privacy enforcement actions?**

    a. **If yes, please detail the average cost of an expert witness used for data privacy enforcement actions, including any factors that could change the cost.**

3. **Chairman Simons, currently, does the Commission utilize an expert witness for data security enforcement actions?**

    a. **If yes, please detail the average cost of an expert witness used for data security enforcement actions, including any factors that could change the cost.**

In answer to questions 2 and 3, the Commission currently employs five technologists, three of whom work full time on privacy and data security matters. These technologists provide expert assistance on privacy and data security cases, for example, by helping attorneys draft discovery requests, participating in meetings with opposing parties, assisting staff in better understanding technical issues, and reviewing pleadings for technical accuracy. In addition, the Commission currently employs a consulting expert on data security, who provides advice regarding numerous data security investigations per year. He charges $300 per hour, and we typically use a few hours of his time every month.

The Commission also retains consulting and testifying experts for specific litigation matters. In its three litigated data security cases, the Commission has spent respectively about $2 million, $250,000, and $400,000 on experts, though the third case is not yet complete. Depending on the case, the Commission also would need experts on claim interpretation, who typically charge $250 per hour; experts on surveys and copy tests, who typically charge $675 per hour; experts on harms suffered by consumers, who have charged between $400 and $675 per hour; and experts on data security, who have charged between $150 and $550 per hour.

4. **Chairman Simons, how are Bureau of Economics staff utilized in data security and data privacy cases within the Bureau of Consumer Protection? Please give specific examples of action items in an enforcement case assigned to the Bureau of Economics staff.**

[6] *See* 84 Fed. Reg. 20777 (May 13, 2019); 84 Fed. Reg. 18711 (May 2, 2019); 84 Fed. Reg. 13115 (Apr. 4, 2019).

The Bureau of Economics reviews every complaint or settlement recommendation that the Bureau of Consumer Protection makes on privacy and data security matters, as they do in all enforcement matters. The Bureau of Economics provides a separate recommendation memorandum to the Commission. In some instances, the Bureau of Consumer Protection requests more specific input from staff economists. For example, staff economists may assist Bureau of Consumer Protection staff with drafting discovery requests aimed at determining the amount of harm caused by a particular practice; analyzing, categorizing, and creating statistical samples of consumer complaints; and developing surveys, studies, and/or copy tests, either with Bureau of Consumer Protection staff as part of an investigation or with outside experts during litigation.

5. **Chairman Simons, with respect to violations of an FTC consent order, what authority does the Commission have to hold company executives personally liable for company acts or practices the Commission determines to violate such order?**

    a. **Please identify the specific statute, rule, or regulation that grants the Commission such authority.**

Rule 65(d)(2) of the Federal Rules of Civil Procedure explicitly states that federal court orders bind a party's officers, agents, servants, employees and attorneys. To prevail against a non-party to an order, the Commission must prove that defendants violated a valid, clear, and unambiguous order where they had notice of the order and the ability to comply.[7] Rule 65(d) applies equally to the Commission's administrative orders.[8]

6. **Chairman Simons, with respect to Section 5 of the FTC Act, what authority does the Commission have to hold company executives personally liable for company acts or practices the Commission determines to violate Section 5?**

    a. **Please identify the specific statute, rule, or regulation that grants the Commission such authority.**

Numerous circuit courts have held that an individual officer, director, or employee may be held liable under the FTC Act for a company's unlawful acts or practices, if the FTC proves the necessary level of involvement. Specifically, individual liability for injunctive relief can be established by showing that the individual defendant participated directly in the unlawful practices or had authority to control them. Individual liability for monetary relief can be established by showing that the individual defendant, in addition to meeting the standard for injunctive relief, had actual knowledge of the unlawful conduct, was recklessly indifferent to its unlawfulness, or had an awareness of a high probability of illegality and intentionally avoided learning the truth.[9]

---

[7] *Angiodynamics, Inc. v. Biolitec AG*, 780 F.3d 420, 426 (1st Cir. 2015).

[8] *Reich v. Sea Sprite Boat Co.*, 50 F.3d 413, 417, (7th Cir. 1995) ("Long ago, however, the Supreme Court held that Rule 65(d) simply restates a norm of federal equity practice and therefore is equally germane to orders enforcing decisions of administrative agencies. *Regal Knitware Co. v. NLRB*, 324 U.S. 9, 14 (1945)."

[9] *See, e.g.*, *FTC v. Ross*, 743 F.3d 886, 892-93 (4th Cir. 2014); *FTC v. Direct Mktg. Concepts, Inc.*, 624 F.3d 1, 12 (1st Cir. 2010); *FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1202-07 (10th Cir. 2005); *FTC v. Publ'g Clearing*

7. **Chairman Simons, with respect to trade regulation rules prescribed by the Commission under Section 18 of the FTC Act, what authority does the Commission have to hold company executives personally liable for company acts or practices the Commission determines to violate a trade regulation rule?**

    a. **Please identify the specific statute, rule, or regulation that grants the Commission such authority.**

When the FTC issues a trade regulation rule under Section 18 of the FTC Act, it does so in order to define with specificity acts or practices that are unfair or deceptive within the meaning of Section 5 of the FTC Act. Courts have held that the standard for liability of individual officers, directors, or employees that applies in Section 5 cases, discussed above in response to Question 6, also applies in cases brought to enforce trade regulation rules.[10]

8. **Chairman Simons, some stakeholders have raised concerns with companies naming products or features that arguably misrepresent the product's capability. For example, Tesla has a feature named "Autopilot" that arguably suggests their cars can operate fully autonomously without human intervention. The operation instructions include disclosures around the feature capabilities which are designed only to assist the driver and that the system requires active driver supervision. With respect to naming products that exceed the products capabilities, please answer the following:**

    a. **Does the FTC have any existing authority to address this concern? If so, please identify such authority.**

The FTC has authority to address product names that exceed the product's capability under Section 5 of the FTC Act, which generally prohibits "unfair or deceptive acts or practices in or affecting commerce."[11] As set forth in the FTC's *Deception Policy Statement*, the FTC considers an act or practice to be deceptive if it contains a representation or an omission of information that would be considered material to consumers and that would mislead consumers acting reasonably under the circumstances.[12] In addition, the Commission has long held that making objective claims without a reasonable basis for the claims constitutes a deceptive practice.[13] Whether or not a particular product name conveys a particular performance claim to consumers would be determined on a case-by-case basis. In some cases, extrinsic evidence may

---

House, Inc., 104 F.3d 1168, 1170-71 (9th Cir. 1997); *FTC v. Gem Merch. Corp.*, 87 F.3d 466, 470 (11th Cir. 1996); *FTC v. Amy Travel Serv., Inc.*, 875 F.2d 564, 573-74 (7th Cir. 1989).

[10] *See, e.g.*, *FTC v. Nat'l Bus. Consultants, Inc.*, 781 F. Supp. 1136, 1145 (E.D. La. 1991); *FTC v. Essex Marketing Group, Inc.*, No. 02-cv-3415, 2008 WL 2704918, at *4-6, (E.D.N.Y. July 8, 2008); *FTC v. Wolf*, No. 94-8119-CIV, 1996 WL 812940, at *8 (S.D. Fla. Jan. 31, 1996).

[11] 15 U.S.C. § 45.

[12] *See FTC Policy Statement on Deception, appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).

[13] *FTC Policy Statement Regarding Advertising Substantiation*, 104 F.T.C. 839 (1984), appended to *Thompson Med. Co.*, 104 F.T.C. 648 (1984).

be needed to determine whether consumers acting reasonably would find a particular product name misleading.

b. Could the Commission's deception authority be applied to review such cases?

The Commission's Section 5 authority to prohibit unfair or deceptive practices extends to false or unsubstantiated advertising claims, including claims made through product names.[14]

9. Chairman Simons, what are the limitations on the Commission's existing deception authority with respect to data privacy?

a. Please answer the same question above with respect to data security.

In order to prove that a claim is deceptive under the FTC Act, the Commission must show that the claim has been made, that it is likely to mislead a consumer acting reasonably under the circumstances, and that it is material. Companies often make claims about privacy and data security in their privacy policies. Some defendants have argued that, because consumers do not typically read privacy policies, claims contained therein cannot be material, and therefore cannot be deceptive under the FTC Act. Although prior Commission statements and relevant case law are contrary to this argument,[15] the Commission likely will continue to face continued legal challenges on this issue.

10. Chairman Simons, what are the limitations on the Commission's existing unfairness authority with respect to data privacy?

a. Please answer the same question above with respect to data security.

Defendants in litigation have made several arguments as to the limitations of the FTC's unfairness authority in the areas of privacy and data security. Most of these arguments relate to the first element the FTC needs to prove in unfairness cases: that an act or practice "causes or is likely to cause substantial injury to consumers."[16] First, defendants have argued that certain non-financial and non-physical harms are not "substantial injury," based on legislative history stating that "emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair."[17] Second, they have argued that, in order to prove that a practice is "likely" to cause substantial injury, the FTC must prove that injury is probable, or will occur with a 51% certainty. Third, defendants have argued that the FTC cannot prove that a

---

[14] *See, e.g.*, *Brake Guard Prods., Inc.*, 125 F.T.C. 138 (1998) (Commission challenged claims that aftermarket brake product, "Brake Guard ABS," was an antilock braking system and provided the benefits of same; Commission order banned the use of the term "ABS" in connection with the product)

[15] *See FTC Policy Statement on Deception*, 103 F.T.C. 110, 174 (1984) (*appended to Cliffdale Assocs., Inc.*) (noting several categories of material claims, such as express claims, claims about the central characteristic of a product, and claims that the Defendant intended to make); *see also In the Matter of Novartis*, 1999 FTC LEXIS 63 *38 (May 27, 1999) ("Materiality is not a test of the effectiveness of the communication in reaching large numbers of consumers. It is a test of the likely effect of the claim on the conduct of a consumer who has been reached and deceived.").

[16] 15 U.S.C. 45(n).

[17] *See FTC Policy Statement on Unfairness*, 104 F.T.C. 949, 1070 (1984) (*appended to International Harvester).*

particular practice "caused" a given injury. For example, in a data breach case, it may be difficult to prove that a particular theft of a consumer's identity resulted from the specific breach at issue in the case.[18] The Commission has rejected each of these arguments,[19] and the Third Circuit in the *Wyndham* case has also confirmed that non-financial injury, such as the cost of people's time in dealing with a breach, is cognizable injury under the FTC Act.[20] Nonetheless, we continue to expend significant litigation resources on these issues.

11. Chairman Simons, we know that small businesses have suffered in Europe since the implementation of GDPR, with some reports finding that investments in startups are down 40 percent. Do you have any suggestions for how can we guard against the same happening here with a federal privacy bill, including lessons learned from the public hearings on consumer protection issues in the 21st Century?

Because the GDPR has been in effect for only a year, there is a limited basis upon which researchers and others might draw conclusions about potential effects that the GDPR has had on investments in startups. That said, the FTC's recent *Hearings on Competition and Consumer Protection in the 21st Century* did include discussion of research showing that, in the European Union, the number of venture capital technology deals and the average amount invested per deal declined in the first several months after the GDPR took effect.[21] Researchers have stated their intent to monitor to see whether those observations remain true on a longer-term basis, and whether they reflect correlation or causation. The FTC will keep abreast of such research.

12. Chairman Simons, at the hearing, you indicated that a federal privacy bill should consider State Attorneys General enforcement. Please answer the following questions about state enforcement:

a. Do you agree that any state enforcement action of the federal law should be brought exclusively in federal court?

i. If yes, please explain.

b. Do you agree that the Commission should receive notice from a state prior to state enforcement of the federal privacy bill?

i. If yes, please explain.

c. Do you agree that the Commission should be able to intervene in any civil action brought by a state?

i. If yes, please explain.

---

[18] *See, e.g.*, *LabMD, Inc. v. FTC*, Appellee's Initial Brief, 2017 U.S. 11th Cir. Briefs Lexis 14*, 10-11 (Feb. 9, 2017).
[19] Opinion of the Commission, *In re LabMD*, Docket No. 9357, 2016 FTC Lexis 128*, 59-60 (July 28, 2016).
[20] *FTC v. Wyndham Worldwide Corp., et al.*, 10 F. Supp. 3d 602, 621-22 (D.N.J. 2014).
[21] Jia, Jian and Jin, Ginger Zhe and Wagman, Liad, *The Short-Run Effects of GDPR on Technology Venture Investment* (May 31, 2019), https://ssrn.com/abstract=3278912 or http://dx.doi.org/10.2139/ssrn.3278912.

d. Do you agree that if the Commission initiates a civil or administrative action on against the same defendant under the same circumstances of a state action, that the state action should be stayed pending resolution of the Commission's action?

i. If yes, please explain.

I believe that the Children's Online Privacy Protection Act ("COPPA") provides a useful model for granting concurrent enforcement authority to state attorneys general. Under COPPA, state attorneys general can bring civil actions enforcing the law on behalf of their residents in federal district courts. The law requires that state attorneys general provide the Commission notice and a copy of the complaint before filing an action, unless doing so is infeasible. COPPA also gives the Commission the right to intervene in any civil action brought by a state and, if the Commission has instituted an action against a defendant, the law prohibits any state from filing a civil action against the same defendant for violating COPPA during the pendency of the Commission's action.

This model has been very successful. Multiple states, including Texas, New Jersey, and New York, have brought actions to enforce COPPA, which ultimately improves children's privacy. The other requirements of the COPPA statute help foster greater collaboration between the Commission and the states, and ensure that the law is interpreted in a consistent manner. I would be in favor of a similar approach in any future federal privacy law.

13. Chairman Simons, in the 114th Congress this Committee, on a party line vote with Republicans voting for and Democrats voting against, reported the Data Security and Breach Notification Act of 2015 to the House Floor. Under that bill, the FTC would currently have first offense civil penalty authority for data security incidents like Equifax. Do you still agree, as you did during our oversight hearing held in July 2018, that the FTC would benefit from having civil penalty authority for violations of the Safeguards Rule?

Yes. Financial institutions subject to the GLB Safeguards Rule often maintain highly sensitive personal information of consumers. Financial institutions that are subject to the Safeguards Rule and that do not comply should be subject to civil penalties for first-time violations.

14. Chairman Simons, I appreciate your focus on whether our current consumer protection and competition laws are working as well as they should, especially in this digital world we now live in. That is why I was encouraged when you announced that you would be holding your 21st Century hearings on consumer protection issues, as well as creating the Technology Taskforce. Please answer the following with respect to the Technology Taskforce and hearings:

a. Please explain what the Technology Taskforce is and how you intend to utilize it's activities or findings with respect to data privacy and data security issues.

b. **What is the status of the Technology Taskforce? How many FTEs are dedicated to the Taskforce?**

c. **Do you have any feedback from the 21st Century hearings you can share? If not, do you plan on producing any summary of findings from the hearings?**

d. **Do you have any feedback with respect to the Technology Taskforce you can share?**

The TTF will be a focal point for the Commission's efforts to further develop our legal and economic understanding of technology markets and promote effective antitrust enforcement in this area of the economy. It will provide a natural home for attorneys and economists with a technical background or with significant practical experience in relevant industries.

The primary focus of the TTF is to identify and investigate anticompetitive conduct (including consummated mergers) in markets in which digital technology is an important dimension of competition, such as online platforms, digital advertising, social networking, software, operating systems, and streaming services. Privacy and data security issues will continue to be handled by the Bureau of Consumer Protection, which has similar technology-focused components already in place. The Bureau of Competition will work closely with the Bureau of Consumer Protection on shared issues and concerns, especially in the context of investigations that raise related issues between privacy and data collection.

The TTF currently has 15 attorneys, with plans to hire two additional attorneys and a technologist soon. The TTF is supported by staff throughout the agency, including other technology experts and the Bureau of Economics. As there is no additional funding for personnel, all of the FTEs have come from within the FTEs allotted to the Bureau of Competition. The TTF staff is busy at work, and I expect them to move quickly to identify potential actions for the Commission.

The Commission's *Hearings on Competition and Consumer Protection in the 21st Century* have explored whether broad-based changes in the economy, evolving business practices, new technologies, and international developments might require adjustments to competition and consumer protection law, enforcement priorities, or policy. Several hearings have focused on the role of technology-based platform businesses. The Hearings and related public comments are helping the Commission obtain and evaluate a broad and diverse range of viewpoints from outside experts and interested persons about high-tech business practices.

15. **Chairman Simons, I understand there is an effort to modernize prescription release and delivery with patient portals and electronic health records (EHRs). There are some questions around the prescription verification process under the Contact Lens Rule. Are you soliciting comment about, and open to considering, updates to modernize the Contact Lens Rule to reflect how e-commerce has transformed the marketplace since it's origination?**

The Commission has proposed changes in the May 28, 2019 Supplemental Notice of Proposed Rulemaking ("SNPRM") to reflect advances in technology. Under this proposal, a prescriber, with the patient's verifiable affirmative consent, could provide the patient with a digital copy of the prescription in lieu of a paper copy. Additionally, the proposed Rule would require that sellers provide a mechanism to allow patients to present their prescriptions directly to sellers. Among other options, sellers could use email, text message, or file upload to obtain such prescriptions. Finally, in the December 7, 2016 Notice of Proposed Rulemaking, the Commission made an initial determination that a portal could be used by a prescriber or a patient to provide a contact lens prescription to a seller, which would allow the seller to complete the sale. The Commission will consider comments received in response to this initial determination and the SNPRM and, if appropriate, make changes before issuing a final rule.

16. Chairman Simons, is the Commission aware of any other instances of verification by automated call for other self-administered class 2 and class 3 medical devices? If so, please list those other instances.

The Commission is not aware of other instances where a self-administered class 2 or class 3 medical device can be verified with a medical provider using an automated telephone message.

a. Please provide information on what percentages of verifications are filled through the following methods: fax, electronic means, personal live calls, or automated calls.

The Commission does not have information about the percentage of verifications made through the various permissible methods.

17. Chairman Simons, how many sellers does the Commission audit annually for verification compliance under the Contact Lens Rule?

The Commission does not conduct annual audits of sellers or prescribers for compliance with the verification process. The Commission investigates sellers and prescribers based on complaints received and by monitoring the marketplace.

a. How many of those audits have led to an enforcement action by the Commission?

Since the Rule's passage, the Commission has taken law enforcement action against eleven contact lens sellers alleging violations of the Rule.[22] The settlement orders in these cases have provided injunctive relief that, among other things, prohibited the defendants from: selling contact lenses without obtaining a prescription from a consumer; selling contact lenses without

[22] *U.S. v. Lawrence L. Duskin*, No. 1:18-cv-07359 (N.D. Cal. Dec. 6, 2018); *U.S. v. Kim*, No. 1:11-cv-05723 (E.D.N.Y. Feb 7, 2012); *U.S. v. Royal Tronics, Inc.*, No. No. 0:11-cv-62491 (S.D. Fla. Jan. 27, 2012); *U.S. v. Thy Xuan Ho*, No. 1:11-cv-03419 (D. Minn. Dec. 27, 2011); *U.S. v. Gothic Lens, LLC*, No. 1:11-cv-00159 (N.D. Ga. Feb. 3, 2011); *U.S. v. Jokeshop, LLC*, No. 1:11-cv-11221 (D. Mass. Nov. 29, 2011); *U.S. v. Contact Lens Heaven, Inc.*, No. 0:08-cv-61713 (S.D. Fla. Dec. 3, 2008); *U.S. v. Chapin N. Wright, II*, No. 1:08-cv-11793 (D. Mass. Oct. 31, 2008); *U.S. v. BeWild, Inc.*, No. 2:07-cv-04896 (E.D.N.Y. Dec. 3, 2007); *U.S. v. Pretty Eyes, LLC*, No. 1:07-cv-02462 (D. Colo. Nov. 28, 2007); *U.S. v. Walsh Optical, Inc.*, No. 2:06-cv-03591 (D.N.J. Aug. 30, 2006).

verifying prescriptions by communicating directly with the prescriber; and failing to maintain records of prescriptions and verifications. In addition, the Commission has sent numerous warning letters to both sellers and prescribers who potentially violated the Rule. Staff will continue to monitor the marketplace and, if appropriate, take action.

18. Chairman Simons, in March 2019, the FTC announced that it would be conducting a Section 6(b) study of certain Internet Service Providers. Does the Commission intend to conduct a similar study of consumer-facing content delivery services including social media services, sometimes referred to as "edge providers"?

The Commission regularly uses its authority under Section 6(b) of the FTC Act, which allows it to conduct industry-wide studies. In the past few years alone, we have studied the practices of data brokers and mobile device manufacturers and, as you mention, we currently are undertaking a study of internet service providers. These types of studies are best suited to areas in which we can make apples-to-apples comparisons across a range of companies. We are considering further 6(b) studies in other industries.

19. Chairman Simons, reports have surfaced that a Civil Investigative Demand (CID) has been issued by the Bureau of Competition to companies that run the largest automobile Dealer Management Systems (DMS) arising from an allegation that by improving the security of the DMSs, some companies are now technologically blocked from accessing them. These DMSs house and process dealership and manufacturer inventory, accounting, human resources and marketing information, and also contain financial, personal and sensitive data about consumer purchases and dealer services provided to consumers. As the FTC urge networks to secure personal data in testimony and guidance and other materials, is the Bureau of Competition having conversations with the Bureau of Consumer Protection about the various access issues that can arise with implementing security

The agency does not publicly comment on the substance of any pending law enforcement investigation. I assure you that the Bureau of Competition and the Bureau of Consumer Protection regularly and appropriately work together on issues of common concern.

The Honorable Robert E. Latta (R-OH)

1. **Chairman Simons, the FTC has emphasized for years how important access to WHOIS data is to its online investigative and enforcement work. Domain name providers have begun limiting access to that data because of Europe's privacy law. The FTC's international consumer protection counsel has been documenting how that is hindering consumer protection and cyber security efforts, and the NTIA has called upon ICANN to solve this problem. How important is it that WHOIS access be restored as soon as possible to protect consumers and intellectual property?**

We believe it remains important for ICANN to develop a unified mechanism to enable those with legitimate interests—law enforcement, regulators, cyber security professionals, IP rights holders, and consumers—to obtain access to appropriate domain name registration (WHOIS) information. Contact information for domain name owners has long been one of the key building blocks in website investigations. The loss of ready access to this data due to EU privacy law developments has created obstacles and delays for those investigating illicit internet activities. For example, recent studies of more than 300 cybersecurity "first responders" and law enforcement investigators concluded that the masking of WHOIS information has impaired the ability to blacklist domains that transmit spam and expose internet users to online threats that could have been preemptively stopped, had WHOIS contact information remained available.[23]

We continue to cooperate with our foreign consumer protection and other enforcement counterparts to work towards a standard ICANN system to promptly and lawfully respond to requests for WHOIS information.

2. **Chairman Simons, we want companies of all sizes to protect consumer information, but we do not want new privacy obligations to crush small businesses and benefit big companies. In the 2012 FTC privacy report, the Commission grappled with this specific concern and excluded some small businesses from its recommendations. How do you think we should be addressing this concern?**

To the extent Congress is considering excluding small businesses from privacy legislation, we would suggest focusing not simply on the size of the company, but on the amount and sensitivity of the data the company collects. A company with few employees can collect highly-sensitive data of millions of consumers, and such a company should be subject to privacy rules. As you note, this is the approach the Commission took in its 2012 Privacy Report. We also took a similar approach in our recent Notice of Proposed Rulemaking on the GLB Safeguards Rule, where we proposed requiring all financial institutions to comply with general provisions requiring reasonable security, but suggested imposing more specific requirements on companies that collect data of more than 5,000 consumers.

3. **Chairman Simons, to date companies have failed to adequately explain to consumers how their information is collected, used, and often shared online. I**

[23] *See* Facts & Figures: Whois Policy Changes Impair Blocklisting Defenses, https://www.securityskeptic.com/2019/03/facts-figures-whois-policy-changes-impair-blacklisting-defenses.html.

believe any federal privacy bill must increase transparency. Can you speak to why transparency is important?

Transparency with respect to data collection, use, and sharing practices is important for multiple reasons. First, transparency helps consumers make informed decisions when choosing to provide their data to businesses whose practices align with the consumer's privacy preferences and expectations. Second, transparency promotes competition by enabling consumers to compare and contrast businesses' data practices and enabling businesses to compete based on their willingness and ability to meet consumers' preferences and expectations. Third, transparency promotes accountability by providing a basis for the FTC and other stakeholders to take action to hold businesses accountable if their actual practices do not comport with their claims. Finally, the process of publicly committing to certain data practices serves an important internal accountability function in making sure that company personnel examine and confirm the practices to which they are publicly committing.

4. **Chairman Simons, What data is being collected to determine the impacts of the GDPR in the United States? And does the FTC have a plan to collect data on the potential impacts of the CCPA? If that information is not being studied already, are there plans to study it?**

The FTC is continuing to collect public comments, including empirical research, until June 30, 2019, on the topics the FTC included in its recent *Hearings on Competition and Consumer Protection in the 21st Century*. The questions that the FTC has posted for public comment include:

- How do state, federal, and international privacy laws and regulations, adopted to protect data and consumers, affect competition, innovation, and product offerings in the United States and abroad?
- What are existing and emerging legal frameworks for privacy protection? What are the benefits and drawbacks of each framework?
- Does the need for federal privacy legislation depend on the efficacy of emerging legal frameworks at the state level? How much time is needed to assess their effect?

The final hearing record will help inform future FTC plans to collect additional data to determine the impacts of the GDPR in the United States and the potential impacts of the CCPA as well as other existing or future privacy laws.

The Honorable Michael C. Burgess (R-TX)

1. **Chairman Simons, in December 2016, the FTC issued a Notice of Proposed Rulemaking announcing changes to the Commission's Contact Lens Rule. These changes included a new regulatory requirement for doctors to collect and maintain for 3 years a signed confirmation that a patient received their contact lens prescription. In addition, the proposal did not address illegal sales, including the filling of expired or incorrect prescriptions.**

   On May 2, 2019, the FTC issued a Supplemental Notice of Proposed Rulemaking that kept the confirmation mandate, but allowed digital copies, and only required sellers to provide patient prescription information to prescribers in a slow and deliberate manner, without eliminating the automation of robocalls.

   Last Congress, Congressman Bobby Rush and I led a letter requesting the FTC reevaluate its 2016 proposed rulemaking, requesting the new rule limit the paperwork mandate and improve enforcement of existing provision to combat illegal sales.

   a. **Can you describe why the FTC assesses the requirement to keep prescription confirmation records for 3 years is a necessary improvement upon the Contact Lens Rule?**

The Commission believes that maintaining records of prescription releases for three years will allow staff to investigate potential violations and, where appropriate, bring enforcement actions. The three-year period is consistent with other recordkeeping obligations in the Rule, and the FTC Act has a three-year statute of limitations for bringing enforcement actions pursuant to a rule violation.[24] Additionally, the Commission believes that some prescribers may already retain eye examination records for at least three years due to state requirements or may already keep customer sales receipts for financial recordkeeping purposes. The Commission will consider comments received in response to the May 28, 2019 Supplemental Notice of Proposed Rulemaking ("SNPRM") and, if appropriate, make changes before issuing a final rule.

   b. **Do you anticipate sellers maintaining the ability to exploit prescriber communication rules to fill prescriptions?**

When Congress enacted the Fairness to Contact Lens Consumers Act, it determined that passive verification was necessary to balance the interests of prescription portability and consumer health. Congress was aware that, in some instances, passive verification could allow sellers to sell contact lenses based on an invalid or inaccurate prescription, and that this could potentially lead to health risks. In the SNPRM, the Commission proposed several changes to improve the passive verification process. The Commission proposed that sellers who use automated telephone verification messages would have to: (1) record the entire call and preserve the

[24] 15 U.S.C. § 57b(d).

complete recording; (2) begin the call by identifying it as a prescription verification request made in accordance with the Contact Lens Rule; (3) deliver the verification message in a slow and deliberate manner and at a reasonably understandable volume; and (4) make the message repeatable at the prescriber's option. This proposal would enable prescribers to better fulfill their role as protectors of patients' eye health because prescribers cannot correct and police invalid, inaccurate, and expired prescriptions if they cannot comprehend a seller's verification request.

Additionally, the Commission proposed changes that would increase patients' access to their prescriptions, maintain patient choice and flexibility, and potentially reduce the number of verification requests. Under the proposal, a prescriber, with the patient's verifiable affirmative consent, has the option to provide the patient with a digital copy of the prescription in lieu of a paper copy. Moreover, although the Rule has always required that prescribers, upon request, provide any person designated to act on behalf of the patient with a copy of the patient's valid contact lens prescription, the Rule did not prescribe a time limit within which this copy had to be provided. The Commission proposed requiring that a prescriber respond to requests for an additional copy of a prescription within forty business hours. To facilitate patients' ability to use their prescriptions, another proposed change would require sellers to provide a mechanism that would allow patients to present their prescriptions directly to sellers.

Finally, the Commission proposed amending the prohibition on seller alteration of prescriptions to address concerns about the misuse of passive verification to substitute a different brand and manufacturer of lenses. The proposal requires a seller who makes an alteration to provide a verification request to the prescriber that includes the name of a manufacturer or brand other than that specified by the patient's prescriber. There is a proposed exception if the patient entered that manufacturer or brand on the seller's order form or the patient orally requested it from the seller.

The Commission will consider comments received in response to the SNPRM and, if appropriate, make changes before issuing a final rule.

2. **Chairman Simons, in the 114th Congress this Committee, on a party line vote with Republicans voting for and Democrats voting against, reported the Data Security and Breach Notification Act of 2015 to the House Floor. Under that bill, the FTC would currently have first offense civil penalty authority for data security incidents, including the Equifax breach.**

    a. **Do you still agree, as you did during our oversight hearing in 2018, that the FTC would benefit from having civil penalty authority for violations of the Safeguards Rule?**

Yes. Financial institutions subject to the GLB Safeguards Rule often maintain highly sensitive personal information of consumers. Financial institutions that are subject to the Safeguards Rule and that do not comply should be subject to civil penalties for first-time violations.

3. **Chairman Simons, when the FTC enjoyed broad rulemaking authority in the 1970s it got so bad that a Democratic-led Congress cut funding to the Commission for several days.**

    a. **How should the events of the past inform our discussion about FTC rulemaking today and under future administrations**

Since the 1970s, Congress has enacted numerous laws that give the FTC discrete rulemaking authority in a variety of areas—children's privacy, privacy and data security for financial institutions, email marketing, telemarketing sales, and contact lens prescriptions, to name just a few. The FTC has exercised that rulemaking authority judiciously. In addition, rulemaking in all of these areas is subject to the procedural protections provided by the Administrative Procedure Act—including public notice and comment, a requirement that the Commission explain its reasoning, and an opportunity for judicial review. In its hearing testimony, the Commission requested similarly targeted APA rulemaking authority for consumer privacy and data security.

Since 1992, the FTC has also maintained a robust regulatory review program. All FTC rules and guides are reviewed periodically to ensure they are up to date, effective, and not overly burdensome. As part of the review process, the FTC solicits public input on issues such as the rule's economic impact; whether there is a continuing need for the rule; whether the rule may conflict with state, local, or other federal laws or regulations; and whether the rule has been affected by any technological, economic, or other industry changes. Decades of experience with targeted rulemaking and regulatory reviews have given the FTC a thorough understanding of rules' regulatory and economic impact, and will continue to inform the FTC's actions in the future.

4. **Chairman Simons, we know that small businesses have suffered in Europe since the implementation of the General Data Protection Regulation (GDPR). In fact, according to some reports, investments in startups are down an astounding 40 percent.**

    a. **How can we guard against the same happening here?**

Because the GDPR has been in effect for only a year, there is a limited basis upon which researchers and others might draw conclusions about potential effects that the GDPR has had on investments in startups. That said, the FTC's recent *Hearings on Competition and Consumer Protection in the 21st Century* did include discussion of research showing that, in the European Union, the number of venture capital technology deals and the average amount invested per deal declined in the first several months after the GDPR took effect. Researchers have stated their intent to monitor to see whether those observations remain true on a longer-term basis, and whether they reflect correlation or causation. The FTC will keep abreast of such research.

<u>The Honorable Richard Hudson (R-NC)</u>

1. **In an article dated May 2, 2019, the Wall Street Journal reported that Facebook is interested in entering the payments and remittances markets as the company "aims to burrow more deeply into the lives of its users." The article also notes that one-third of the world's population logs on to Facebook on a monthly basis.**

    a. **Given Facebook's track record with consumer data, what concerns would FTC have if Facebook gained access to billions of people's sensitive financial data?**

The Commission has confirmed a non-public investigation into Facebook. It would be inappropriate to comment on potential practices of a company under investigation.

    b. **Given the potential scale of this business, what competition issues does FTC foresee? How will the FTC assure that other services will be able to compete against the likes of a Facebook?**

The Bureau of Competition recently announced the creation of a Technology Task Force ("TTF") that will enhance the Commission's antitrust focus on technology-related ecosystems, including technology platforms as well as markets for online advertising, social networking, mobile operating systems, and apps. The TTF will monitor competition in U.S. technology markets, investigate any conduct in these markets that may harm competition, and, when warranted, take actions to ensure that consumers benefit from free and fair competition.

2. **TechCrunch blog post entitled "Facebook is Pivoting" suggested that Facebook's recent moves indicate that it will evolve into a private end-to-end encryption platform for communication and commerce. The blog states that what "Facebook really wants next is for Messenger to become... an impregnable walled garden, used for business communications as well as personal, which dominates not just messaging but commerce." A situation "in which Instagram is the king of all social media, while Messenger/WhatsApp rule messaging, occupy the half-trillion dollar international-remittances space, and also take basis points from millions of daily transactions performed on" Facebook's platforms.**

    a. **As Facebook Inc. seeks to leverage its owned platforms to offer financial and other services, how is the FTC going to ensure Facebook responsibly manages this evolution into a financial and e-commerce giant?**

    b. **Given that Facebook touches one-third of the world's population and nearly two-thirds of all Americans, does the FTC have confidence Facebook will handle this evolution properly, given the company's history of handling sensitive data?**

The Commission has confirmed a non-public investigation into Facebook. It would be inappropriate to comment on potential practices of a company under investigation.

Additional Questions for the Record

Subcommittee on Consumer Protection and Commerce
Hearing on
"Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security"
May 8, 2019

The Honorable Christine S. Wilson, Commissioner
The Federal Trade Commission

The Honorable Jan Schakowsky (D-IL)

1. **On June 11, 2019, the Federal Trade Commission (FTC) will hold a workshop on online event tickets. I have heard reports of a number of consumer protection issues concerning online event tickets that raise serious concerns and I hope the FTC will consider addressing these issues during its workshop. For example, I have heard concerns that primary ticket platforms have begun forcing purchasers to disclose personally identifiable information by creating an account with the primary ticket seller to use a ticket, even when tickets are resold on a secondary market. I have also heard complaints about primary ticket sellers that hold tickets back from the market pursuant to agreements with venues, artists, or other partners. In addition, I have received complaints about primary ticket vendors putting technological restrictions on the transfer of tickets, which can prevent ticket holders from reselling or giving away tickets if they cannot attend the event.**

    a. **Will the FTC examine these issues at its upcoming hearing on online event tickets?**

Yes, the June 11 Online Event Ticketing Workshop will examine the issues that you raise and their possible impact on consumers in the online event tickets marketplace.

    b. **Has the FTC received similar complaints from consumers?**

The most common consumer complaints we receive about online event ticketing concern hidden or inadequately disclosed ticketing fees in the primary and secondary markets, and consumers who report ticket resellers misled them to believe they were purchasing tickets from the venue or authorized seller at face value (when in fact they were purchasing tickets from resellers at a significant markup). The Commission also received several thousand consumer comments in connection with the upcoming ticketing workshop. Those comments overwhelmingly concerned hidden or inadequately disclosed ticketing fees and/or the high cost of such fees. The FTC has received consumer complaints or comments regarding the practices you outline, but they are not as prevalent.

c. Do you agree that, if true, these practices raise concerns about unfair or deceptive practices in the market for online event tickets?

These practices may raise questions about transparency and consumer understanding in the online event tickets marketplace; however, it is unclear whether requiring ticket buyers to provide personally identifying information, holding back tickets for later sale, or restricting the transfer of tickets are unfair or deceptive acts or practices under Section 5 of the FTC Act.

The Honorable Bobby L. Rush (D-IL)

1. **In 2014, the Federal Trade Commission (FTC) published a report called "Data Brokers: A Call for Transparency and Accountability" that shed light on the secretive world of data brokers that buy and sell vast amounts of consumer personal information, often entirely behind the scenes. The FTC's report called on Congress to pass legislation that would require data brokers to be more transparent and give consumers the right to opt-out, among other things.**

    a. **Do you still agree that Congress should pass legislation addressing data brokers?**

The current Commission has not taken a position on data broker legislation specifically. It has supported federal privacy and security legislation that would give the Commission authority to seek civil penalties for first-time privacy and security violations; conduct targeted APA rulemaking; and exercise jurisdiction over common carriers and non-profit entities. I am concerned about data broker collection, use, and sale of sensitive consumer information and encourage Congress to consider data broker practices in conjunction with its deliberations regarding federal privacy legislation.

2. **While innovation in the tech industry is having a tremendous impact on our economy and the lives of everyday Americans, it is also creating new challenges in protecting consumers and competitive markets. I have heard reports of certain online platforms giving their subsidiary businesses preferential treatment over their competitors.**

    a. **Are you looking into anti-consumer and anti-competitive behaviors of this nature?**

    b. **In your opinion, does the FTC currently have the authority and capacity to curtail this behavior?**

As more and more of the nation's commerce takes place on online platforms, the operation of these platforms has received increased scrutiny by both the public and the antitrust agencies. I believe the FTC has many of the tools it needs to protect consumers online, although I have called for Congress to consider giving the FTC the authority to seek civil penalties for initial privacy violations, which would create an important deterrent effect. Moreover, I believe consumers would benefit if the FTC had broader enforcement authority to take action against common carriers and nonprofits, which it cannot currently do under the FTC Act. That said, you can be assured that the agency is vigilant in its oversight of the internet economy, and we will not hesitate to take strong and appropriate action against any act or practice that violates any statute that we enforce.

Given the growing importance of high-technology industries, the FTC's Bureau of Competition recently announced the creation of a Technology Task Force that will enhance the Commission's antitrust focus on technology-related ecosystems, including technology platforms and markets for online advertising, social networking, mobile operating systems, and apps. The task force

will monitor competition in U.S. technology markets, investigate any conduct in these markets that may harm competition, and, when warranted, take actions to ensure that consumers benefit from competition.

The FTC does not publicly comment on pending law enforcement investigations. As a general matter, however, I can say that the U.S. antitrust laws prohibit certain kinds of conduct that harm consumers by diminishing competition. Some conduct, like price-fixing, is so pernicious that it is condemned as *per se* unlawful without an elaborate inquiry. In the remaining cases, however, we must conduct a fact-specific inquiry to assess whether the challenged conduct is, on net, anticompetitive. ,I look forward to supporting the work of the task force as it conducts its analysis of these issues.

3. **As all of you know, robocalls are extremely burdensome on consumers and every effort needs to be taken to ensure that consumers are not being taken advantage of by these unscrupulous actors. I am also concerned by the reports I have heard that robocalls are now being used by online contact lens retailers to usurp the verification of contact lens prescriptions, placing consumers at an even greater risk of receiving the wrong Class II or III medical devices.**

    a. **Do you agree that efforts need to be taken to update the passive verification process?**

When Congress enacted the Fairness to Contact Lens Consumers Act ("FCLCA"), it determined that passive verification was necessary to balance the interests of prescription portability and consumer health. Congress was aware that passive verification could, in some instances, allow sellers to sell contact lenses based on an invalid or inaccurate prescription, and that this could potentially lead to health risks. In the May 28, 2019 Supplemental Notice of Proposed Rulemaking ("SNPRM"), the Commission proposed several changes to improve the passive verification process. The Commission proposed that sellers who use automated telephone verification messages would have to: (1) record the entire call and preserve the complete recording; (2) begin the call by identifying it as a prescription verification request made in accordance with the Contact Lens Rule; (3) deliver the verification message in a slow and deliberate manner and at a reasonably understandable volume; and (4) make the message repeatable at the prescriber's option. This proposal enables prescribers to fulfill their role as protectors of patients' eye health because prescribers cannot correct and police invalid, inaccurate, and expired prescriptions if they cannot comprehend a seller's verification request.

Additionally, the Commission proposed changes that would increase patients' access to their prescription, maintain patient choice and flexibility, and potentially reduce the number of verification requests. Under the proposal, a prescriber, with the patient's verifiable affirmative consent, has the option to provide the patient with a digital copy of the prescription in lieu of a paper copy. Moreover, although the Rule has always required that prescribers, upon request, provide any person designated to act on behalf of the patient with a copy of the patient's valid contact lens prescription, the Rule did not prescribe a time limit in which this copy had to be provided. The Commission proposed requiring that a prescriber respond to requests for an additional copy of a prescription within forty business hours. To facilitate patients' ability to use

their prescriptions, another proposed change would require sellers to provide a mechanism that would allow patients to present their prescriptions directly to sellers.

Finally, the Commission proposed amending the prohibition on seller alteration of prescriptions to address concerns about the misuse of passive verification to substitute a different brand and manufacturer of lenses. The proposal requires a seller who makes an alteration to provide a verification request to the prescriber that includes the name of a manufacturer or brand other than that specified by the patient's prescriber. There is an exception if the patient entered that manufacturer or brand on the seller's order form or the patient orally requested it from the seller.

The Commission will consider comments received in response to the SNPRM and, if appropriate, make changes before issuing a final rule.

b. Do you agree that robocalls need to be eliminated from use within the passive verification system?

An effective verification process enables prescribers, when necessary, to prevent improper sales and allows sellers to provide consumers with their prescribed contact lenses without delay. The FCLCA expressly permits telephone communication for verification and the Commission believes it would be contrary to Congressional intent to prohibit use of automated technology for the purpose of prescription verification. The Commission does not have empirical data showing the frequency of incomplete or incomprehensible automated telephone messages or that a phone call with an automated message is necessarily less reliable than one with a live person. The evidence suggests that these calls can be an efficient method of verification. However, the Commission recognizes the burden on prescribers and potential health risk to patients from incomplete or incomprehensible automated telephone messages. As described in response to question 3.a, the Commission has proposed changes to automated telephone messages that would improve the verification process.

c. Could you support updating the Fairness to Contact Lens Consumers Act to eliminate robocalls and update the passive verification system to include secured emails and patient portals to verify and document contact lens prescription verification?

Under the current Rule, a "seller may sell contact lenses only in accordance with a contact lens prescription for the patient that is: (1) Presented to the seller by the patient or prescriber directly or by facsimile; or (2) Verified by direct communication." 16 C.F.R. § 315.5(a). Because the Rule's definition of direct communication already includes electronic mail, a seller and a prescriber could use email during the verification process. In the December 7, 2016 Notice of Proposed Rulemaking ("NPRM"), the Commission made an initial determination that a portal could be used by a prescriber or a patient to "directly" present a contact lens prescription to a seller. The Commission will consider comments received in response to this initial determination and, if appropriate, make changes before issuing a final rule.

4. In December 2016, the FTC issued a Notice of Proposed Rulemaking to update the Contact Lens Rule. As a part of this process, providers and manufacturers of

contact lenses urged the FTC to require common-sense changes to the current contact lens market, including quantity limits and ways to update methods of communication under the passive verification process. The FTC responded by stating that there was insufficient evidence that consumers are buying excessive quantities of contact lenses and that it did not have the statutory authority to update the passive verification process.

a. Do you support efforts to ensure patient safety regarding the current proposed rulemaking process that will include patients only receiving contact lenses as prescribed under the valid prescription?

Federal law does not permit a seller to sell contact lenses to a patient unless the seller has obtained a copy of the prescription or verified the patient's prescription information with the prescriber. The SNPRM's proposed changes improve patient access to contact lens prescriptions and address concerns with the passive verification requests and alterations by sellers.

5. **Last May, Rep. Michael Burgess (R-TX) and I led a letter to the FTC that laid out several concerns we have regarding the FTC rulemaking process around the Fairness to Contact Lens Consumers Act. In total, over 50 members of Congress signed this letter where we discussed the lack of enforcement action by the FTC to address the illegal sales of contact lenses and the burdensome new requirements on eye care providers.**

a. Has the FTC investigated or independently audited any online sellers to determine the number of lenses provided to patients?

The Commission has not audited online sellers to determine the number of lenses provided to patients. Staff has investigated specific complaints of illegal sales related to excessive quantities. We will continue to monitor the marketplace, taking action against violations as appropriate.

b. What enforcement mechanisms has the FTC used to ensure that sellers are not enabling the circumvention of state laws governing prescription renewal or harming patients by providing excessive numbers of contact lenses?

In the NPRM, the Commission considered the issue of patients purchasing excessive quantities of contact lenses. Although concerned with anecdotal reports, the Commission concluded that the evidence did not show that the sale of excessive amounts of contact lenses is a widespread problem.[1] Furthermore, a prescriber who receives a verification request for an excessive amount of lenses can contact the seller to prevent the sale from being completed.

The Commission recently has taken enforcement action with respect to unlawful conduct by a seller. Specifically, the Commission recently announced an enforcement action against a contact lens seller challenging the sale of contact lenses without a valid prescription. The order banned

[1] NPRM at 88549-50; *see also* Vision Council, U.S. Optical Market Eyewear Overview 13 (2018), https://www.ftc.gov/sites/default/files/filefield_paths/steve_kodey_ppt_presentation.pdf (noting that 82% of contact lens users had an eye exam within the last 12 months and over 95% had an exam within the last two years)

the defendant from selling contact lens and imposed a $575,000 civil penalty. *U.S. v. Duskin*, No. 1:18-cv-07359 (N.D. Cal. Dec. 6, 2018).

How often has the FTC acted on this important safety issue?

As discussed in the response to question 5.b, the Commission does not believe that the evidence shows that excessive sale of contact lenses is a widespread problem. However, the Commission recognizes the importance of patient safety. Staff will continue to monitor the marketplace and, if appropriate, take action.

6. **Many businesses are increasingly dependent on digital platforms that they do not own or operate to connect with customers.**

    a. **With current statutory authorities in mind, what can be done to protect consumers if companies that operate these platforms offer subsidiary business products and restrict or disadvantage competitors with similar businesses on these platforms? What is the FTC doing to curtail it?**

    b. **One example of how a platform operator might harm consumers is by prohibiting businesses from communicating with their customers through that platform. Do you believe that this sort of behavior must be addressed and, if so, does the FTC currently have the statutory authority to do so?**

Please see the answer to question 2.

7. **It has been brought to my attention that the leading internet browser has been considering a major change in what type of information is available to consumers in their product, reducing the available information that consumers use to defend themselves against a host of online threats like phishing and content spoofing.**

    a. **As the agency charged with protecting our nation's consumers and enforcing our data privacy laws, do you have concerns about what this practice means for consumers and their data privacy and security?**

    b. **Have you discussed this issue with the browsers or asked them to explain their changes and how they will impact consumer safety online? If not, do you intend to?**

Consumers' secure online experiences depend on many factors, and the ecosystem continues to evolve quickly. The Commission is committed to promoting consumer safety online and will monitor these changes to evaluate whether they are likely to harm consumers.

In addition to our enforcement work, detailed in the Commission's written testimony, we engage in extensive consumer education, examples of which you may find here: https://www.consumer.ftc.gov/articles/0009-computer-security.

The Honorable Robert E. Latta (R-OH)

1. **Commissioner Wilson, to date companies have failed to adequately explain to consumers how their information is collected, used, and often shared online. I believe any federal privacy bill must increase transparency.**

    a. **Can you speak to why transparency is important?**

Transparency with respect to data collection, use, and sharing practices is important for multiple reasons. First, transparency helps to facilitate informed decisions whereby a consumer can choose to provide their data to those businesses whose data practices comport with the consumer's preferences and expectations. Second, transparency promotes competition by enabling consumers to compare and contrast businesses' data practices and enabling businesses to compete based on their willingness and ability to meet consumers' preferences and expectations. Third, transparency promotes accountability by providing a basis for the FTC and other stakeholders to be able to take action to hold businesses accountable if their actual practices do not comport with their stated practices. Finally, the process of publicly committing to data practices serves an important internal purpose. This process typically requires companies to examine and confirm their practices to ensure compliance with public commitments.

Additional Questions for the Record

Subcommittee on Consumer Protection and Commerce
Hearing on
"Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security"
May 8, 2019

The Honorable Rebecca Kelly Slaughter, Commissioner
The Federal Trade Commission

The Honorable Jan Schakowsky (D-IL)

1. **On June 11, 2019, the Federal Trade Commission (FTC) will hold a workshop on online event tickets. I have heard reports of a number of consumer protection issues concerning online event tickets that raise serious concerns and I hope the FTC will consider addressing these issues during its workshop. For example, I have heard concerns that primary ticket platforms have begun forcing purchasers to disclose personally identifiable information by creating an account with the primary ticket seller to use a ticket, even when tickets are resold on a secondary market. I have also heard complaints about primary ticket sellers that hold tickets back from the market pursuant to agreements with venues, artists, or other partners. In addition, I have received complaints about primary ticket vendors putting technological restrictions on the transfer of tickets, which can prevent ticket holders from reselling or giving away tickets if they cannot attend the event.**

    a. **Will the FTC examine these issues at its upcoming hearing on online event tickets?**

Yes, the June 11 Online Event Ticketing Workshop examined the issues that you raised and their possible impact on consumers in the online event tickets marketplace. In my opening remarks, I called for industry to adopt all-in upfront pricing to limit sticker shock and improve consumers' ability to comparison shop. Should industry fail to do so, government intervention may be appropriate. The written and audio-visual record of the workshop is available at: https://www.ftc.gov/news-events/events-calendar/2019/03/online-event-tickets-workshop.

    b. **Has the FTC received similar complaints from consumers?**

The most common consumer complaints we receive about online event ticketing concern hidden or inadequately disclosed ticketing fees in the primary and secondary markets, and consumers who report ticket resellers misled them to believe they were purchasing tickets from the venue or authorized seller at face value (when in fact they were purchasing tickets from resellers at a significant markup). The Commission also received several thousand consumer comments in connection with the recent ticketing workshop. Those comments overwhelmingly concerned

hidden or inadequately disclosed ticketing fees or the high cost of such fees. I am concerned that in many cases the fee disclosures can happen only after the consumer creates an account and thereby provides PII. And I share concerns about creating artificial scarcity—whether it is through the venue's practice of holding tickets back or the unscrupulous use of bots—to create artificially high prices for tickets. These issues, in addition to the ones you raise, should be the focus of continued Commission investigatory attention.

c. Do you agree that, if true, these practices raise concerns about unfair or deceptive practices in the market for online event tickets?

The practices you raise and others discussed at the ticket workshop make clear that the ticket market is not functioning well for consumers. In my opening remarks at the workshop, I called for a federal solution to the problem of bait-and-switch fees that add 30% to the cost of the ticket on the final check-out screen, long after a consumer has signed in, selected seats, and sometimes entered credit card information. Consumers deserve and demand all-in upfront pricing for live events, just as airlines are required to provide by federal rule. I was pleased that in the panel on the subject, representatives from SeatGeek, StubHub, Eventbrite, and Ticketmaster all stated that they would support a federal standard that requires all-in upfront pricing for tickets.

In addition to the consumer protection matters you raise, we must also think carefully about competition concerns in the ticketing market. If the ticket marketplace is not functioning competitively, consumers will never be adequately protected.

The Honorable Bobby L. Rush (D-IL)

1. **In 2014, the Federal Trade Commission (FTC) published a report called "Data Brokers: A Call for Transparency and Accountability" that shed light on the secretive world of data brokers that buy and sell vast amounts of consumer personal information, often entirely behind the scenes. The FTC's report called on Congress to pass legislation that would require data brokers to be more transparent and give consumers the right to opt-out, among other things.**

    a. **Do you still agree that Congress should pass legislation addressing data brokers?**

Yes. The FTC's call for legislation that would require data brokers to be more transparent and give consumers more control over the collection and sharing of their data is just as critical now as it was in 2014—if not more so. In the 2014 report, the Commission found that there was "a fundamental lack of transparency about data broker industry practices. Data brokers acquire a vast array of detailed and specific information about consumers; analyze it to make inferences about consumers, some of which may be considered sensitive; and share the information with clients in a range of industries. All of this activity takes place behind the scenes, without consumers' knowledge." In the five years that have passed since the FTC issued its report, the industry has only grown more opaque—while reaching even more consumer data. I am concerned that non-consumer facing entities such as data brokers, ad networks and analytics companies are operating with near total impunity—invisible to consumers and clouded to regulators.

2. **While innovation in the tech industry is having a tremendous impact on our economy and the lives of everyday Americans, it is also creating new challenges in protecting consumers and competitive markets. I have heard reports of certain online platforms giving their subsidiary businesses preferential treatment over their competitors.**

    a. **Are you looking into anti-consumer and anti-competitive behaviors of this nature?**

I share your concern about the importance of protecting American consumers and competition in technology markets. In February, the FTC announced the creation of a Technology Task Force, a team that is intensely focused addressing competition in the technology industry. While I cannot publicly comment on any pending law enforcement investigations or confirm the existence of any investigations, I believe the Commission should be and is committed to investigating alleged anticompetitive conduct and taking strong action when it finds violations.

    b. **In your opinion, does the FTC currently have the authority and capacity to curtail this behavior?**

The FTC enforces Section 5 of the FTC Act, which gives it the authority to investigate and challenge "unfair methods of competition." The antitrust statutes are purposely broad and intended to cover evolving patterns of conduct or market structure; however, especially in light

of recent jurisprudence, the burden on the government to succeed in court is high. Under current Section 5 jurisprudence, the conduct you identify would likely be subject to a "rule of reason" analysis and require a fact-intensive investigation into whether the anticompetitive effects of the conduct outweigh the procompetitive justifications. We should always be using our existing statutory authority to its maximum effectiveness, and we should not be afraid to bring hard or novel cases. That said, it may be worthwhile for Congress to consider legislation to correct problematic court decisions. An even more pressing problem than constraints on our statutory authority, however, is constraints on our resources. Over the past 30 years, FTC funding has not kept pace with the demands placed on it as a result of the expansion of our economy, the volume of merger activity, and the resource intensity of merger review and litigation. The Commission is always looking for ways to use existing resources more efficiently, but additional resources would be put to good use and help us to do more to further our competition and consumer protection missions.

3. **As all of you know, robocalls are extremely burdensome on consumers and every effort needs to be taken to ensure that consumers are not being taken advantage of by these unscrupulous actors. I am also concerned by the reports I have heard that robocalls are now being used by online contact lens retailers to usurp the verification of contact lens prescriptions, placing consumers at an even greater risk of receiving the wrong Class II or III medical devices.**

    a. **Do you agree that efforts need to be taken to update the passive verification process?**

When Congress enacted the Fairness to Contact Lens Consumers Act ("FCLCA"), it determined that passive verification was necessary to balance the interests of prescription portability and consumer health. Congress was aware that passive verification could, in some instances, allow sellers to sell contact lenses based on an invalid or inaccurate prescription, and that this could potentially lead to health risks. In the May 28, 2019 Supplemental Notice of Proposed Rulemaking ("SNPRM"), the Commission proposed several changes to improve the passive verification process. The Commission proposed that sellers who use automated telephone verification messages would have to: (1) record the entire call and preserve the complete recording; (2) begin the call by identifying it as a prescription verification request made in accordance with the Contact Lens Rule; (3) deliver the verification message in a slow and deliberate manner and at a reasonably understandable volume; and (4) make the message repeatable at the prescriber's option. This proposal enables prescribers to fulfill their role as protectors of patients' eye health because prescribers cannot correct and police invalid, inaccurate, or expired prescriptions if they cannot comprehend a seller's verification request.

Additionally, the Commission proposed changes that would increase patients' access to their prescription, maintain patient choice and flexibility, and potentially reduce the number of verification requests. Under the proposal, a prescriber, with the patient's verifiable affirmative consent, has the option to provide the patient with a digital copy of the prescription in lieu of a paper copy. Moreover, although the Rule has always required that prescribers, upon request, provide any person designated to act on behalf of the patient with a copy of the patient's valid contact lens prescription, the Rule did not prescribe a time limit in which this copy had to be provided. The Commission proposed requiring that a prescriber respond to requests for an

additional copy of a prescription within forty business hours. To facilitate patients' ability to use their prescriptions, another proposed change would require sellers to provide a mechanism that would allow patients to present their prescriptions directly to sellers, including electronically.

The Commission will consider comments received in response to the SNPRM and, if appropriate, make changes before issuing a final rule.

b. Do you agree that robocalls need to be eliminated from use within the passive verification system?

No. While I share your concern about robocalls that target and irritate consumers, the robocalls in question here do not go to individual consumers or personal cell phones; they go to the business lines of contact lens prescribers. An effective verification process enables prescribers, when necessary, to prevent improper sales and allows sellers to provide consumers with their prescribed contact lenses without delay. The FCLCA expressly permits telephone communication for verification, and the Commission believes it would be contrary to Congressional intent to prohibit use of automated technology for the purpose of prescription verification. The Commission does not have empirical data showing the frequency of incomplete or incomprehensible automated telephone messages or that a phone call with an automated message is necessarily less reliable than one with a live person. The evidence suggests that these calls can be an efficient method of verification. Still, the Commission recognizes the burden on prescribers and potential health risk to patients from incomplete or incomprehensible automated telephone messages. As described in response to question 3.a, the Commission has proposed changes to automated telephone messages that would improve the verification process.

c. Could you support updating the Fairness to Contact Lens Consumers Act to eliminate robocalls and update the passive verification system to include secured emails and patient portals to verify and document contact lens prescription verification?

Under the current Rule, a "seller may sell contact lenses only in accordance with a contact lens prescription for the patient that is: (1) Presented to the seller by the patient or prescriber directly or by facsimile; or (2) Verified by direct communication." 16 C.F.R. § 315.5(a). Because the Rule's definition of direct communication already includes electronic mail, a seller and a prescriber could use email during the verification process. In the December 7, 2016 Notice of Proposed Rulemaking ("NPRM"), the Commission made an initial determination that a portal could be used by a prescriber or a patient to "directly" present a contact lens prescription to a seller. The Commission will consider comments received in response to this initial determination and, if appropriate, make changes before issuing a final rule.

4. **In December 2016, the FTC issued a Notice of Proposed Rulemaking to update the Contact Lens Rule. As a part of this process, providers and manufacturers of contact lenses urged the FTC to require common-sense changes to the current contact lens market, including quantity limits and ways to update methods of communication under the passive verification process. The FTC responded by stating that there was insufficient evidence that consumers are buying excessive**

quantities of contact lenses and that it did not have the statutory authority to update the passive verification process.

a. Do you support efforts to ensure patient safety regarding the current proposed rulemaking process that will include patients only receiving contact lenses as prescribed under the valid prescription?

The FCLCA reflects Congress's understanding of the need to prioritize both patient safety and access to affordable contact lenses. The Commission does not believe patients should be able to purchase contacts without a valid prescription. The SNPRM's proposed changes improve patient access to contact lens prescriptions and address concerns with the passive verification requests and alterations by sellers. Speaking for myself, I am interested in learning from comments in answer to the questions asked in the SNPRM how often a prescriber's election of brand or manufacturer is based on medical judgment about the ocular health of the patient (for example, the patient's astigmatism requires toric lenses). I am also interested in learning, for circumstances in which a prescriber elects a brand or manufacturer for reasons other than medical judgment about ocular health, what reasons inform the selection and whether it is common for a patient to test the fit of more than one material, brand, or manufacturer before receiving a prescription. In such circumstances, I am concerned about whether a consumer is able to make an informed choice among competing sellers.

5. **Last May, Rep. Michael Burgess (R-TX) and I led a letter to the FTC that laid out several concerns we have regarding the FTC rulemaking process around the Fairness to Contact Lens Consumers Act. In total, over 50 members of Congress signed this letter where we discussed the lack of enforcement action by the FTC to address the illegal sales of contact lenses and the burdensome new requirements on eye care providers.**

a. Has the FTC investigated or independently audited any online sellers to determine the number of lenses provided to patients?

I am not aware of any Commission audits of online sellers to determine the number of lenses provided to patients.

b. What enforcement mechanisms has the FTC used to ensure that sellers are not enabling the circumvention of state laws governing prescription renewal or harming patients by providing excessive numbers of contact lenses?

In the 2016 NPRM, the Commission considered the issue of patients' purchasing excessive quantities of contact lenses. Although concerned by anecdotal reports, the Commission concluded that the evidence did not show that the sale of excessive amounts of contact lenses is a widespread problem.[1] Furthermore, a prescriber who receives a verification request for an excessive amount of lenses can contact the seller to prevent the sale from being completed. Staff

[1] *See* Fed. Trade Comm'n, Contact Lens Rule, Notice of Proposed Rulemaking, 81 Fed. Reg. 88526, 88549–50 (Dec. 7, 2016); *see also* Vision Council, U.S. Optical Market Eyewear Overview 13 (2018), https://www.ftc.gov/sites/default/files/filefield_paths/steve_kodey_ppt_presentation.pdf (noting that 82% of contact lens users had an eye exam within the last 12 months and over 95% had an exam within the last two years).

has investigated and will continue to investigate specific complaints of illegal sales related to excessive quantities. We will continue to monitor the marketplace, taking action against violations as appropriate.

c. How often has the FTC acted on this important safety issue?

As discussed in the response to question 5.b, the Commission does not believe that the evidence shows that excessive sale of contact lenses is a widespread problem. Because the Commission recognizes the importance of patient safety, staff will continue to monitor the marketplace and, if appropriate, take action.

6. Many businesses are increasingly dependent on digital platforms that they do not own or operate to connect with customers.

a. With current statutory authorities in mind, what can be done to protect consumers if companies that operate these platforms offer subsidiary business products and restrict or disadvantage competitors with similar businesses on these platforms? What is the FTC doing to curtail it?

Under current Section 5 jurisprudence, the conduct you identify would likely be subject to a "rule of reason" analysis and require a fact-intensive investigation into whether the anticompetitive effects of the conduct outweigh the procompetitive justifications. In February, the FTC announced the creation of a Technology Task Force, a team that is intensely focused on addressing competition in the technology industry. While I cannot publicly comment on any pending law enforcement investigations or confirm the existence of any investigations, I believe the Commission is committed to investigating alleged anticompetitive conduct and taking strong action when it finds violations of the law.

b. One example of how a platform operator might harm consumers is by prohibiting businesses from communicating with their customers through that platform. Do you believe that this sort of behavior must be addressed and, if so, does the FTC currently have the statutory authority to do so?

The Commission must closely scrutinize mergers and conduct in technology markets. The FTC enforces Section 5 of the FTC Act, which gives it the authority to investigate and challenge "unfair methods of competition." Under current Section 5 jurisprudence, the conduct you identify would likely be subject to a "rule of reason" analysis and require a fact-intensive investigation into whether the anticompetitive effects of the conduct outweigh the procompetitive justifications.

The antitrust statutes are purposely broad and intended to cover evolving patterns of conduct or market structure; however, especially in light of recent jurisprudence, the burden on the government to succeed in court is high. We should always be using our existing statutory authority to its maximum effectiveness, and we should not be afraid to bring hard or novel cases. That said, it may be worthwhile for Congress to consider legislation to correct problematic court decisions and decrease the burden on the agency.

An even more pressing problem than constraints on our statutory authority, however, is constraints on our resources. Over the past 30 years, FTC funding has not kept pace with the demands placed on it as a result of the expansion of our economy, the volume of merger activity, and the resource intensity of merger review and litigation. The Commission is always looking for ways to use existing resources more efficiently, but additional resources would be put to good use and help us to do more to further our competition and consumer protection missions.

7. **It has been brought to my attention that the leading internet browser has been considering a major change in what type of information is available to consumers in their product, reducing the available information that consumers use to defend themselves against a host of online threats like phishing and content spoofing.**

    a. **As the agency charged with protecting our nation's consumers and enforcing our data privacy laws, do you have concerns about what this practice means for consumers and their data privacy and security?**

    b. **Have you discussed this issue with the browsers or asked them to explain their changes and how they will impact consumer safety online? If not, do you intend to?**

While it would be imprudent to comment on any particular company or fact pattern, as a general matter I believe the FTC should always carefully scrutinize practices that may harm consumers and pursue appropriate action if the law has been violated. Ensuring that consumers' data privacy and security is protected by the companies they patronize—and on which they depend—is a top priority for me and for the Commission as a whole.

Additional Questions for the Record

Subcommittee on Consumer Protection and Commerce
Hearing on
"Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security"
May 8, 2019

The Honorable Noah Joshua Phillips, Commissioner
The Federal Trade Commission

The Honorable Jan Schakowsky (D-IL)

1. **On June 11, 2019, the Federal Trade Commission (FTC) will hold a workshop on online event tickets. I have heard reports of a number of consumer protection issues concerning online event tickets that raise serious concerns and I hope the FTC will consider addressing these issues during its workshop. For example, I have heard concerns that primary ticket platforms have begun forcing purchasers to disclose personally identifiable information by creating an account with the primary ticket seller to use a ticket, even when tickets are resold on a secondary market. I have also heard complaints about primary ticket sellers that hold tickets back from the market pursuant to agreements with venues, artists, or other partners. In addition, I have received complaints about primary ticket vendors putting technological restrictions on the transfer of tickets, which can prevent ticket holders from reselling or giving away tickets if they cannot attend the event.**

    a. **Will the FTC examine these issues at its upcoming hearing on online event tickets?**

Yes, the June 11 Online Event Ticketing Workshop examined the issues that you raise and their possible impact on consumers in the online event tickets marketplace.

    b. **Has the FTC received similar complaints from consumers?**

The most common consumer complaints we receive about online event ticketing concern hidden or inadequately disclosed ticketing fees in the primary and secondary markets, and consumers who report that ticket resellers misled them to believe they were purchasing tickets from the venue or authorized seller at face value (when in fact they were purchasing tickets from resellers at a significant markup). The Commission also received several thousand consumer comments in connection with the ticketing workshop, which overwhelmingly concerned hidden, inadequately disclosed, or excessive ticketing fees. While the FTC may also have received consumer complaints or comments regarding the practices you outline, they do not appear to be as prevalent.

c. Do you agree that, if true, these practices raise concerns about unfair or deceptive practices in the market for online event tickets?

These practices may raise questions about privacy, transparency, and consumer understanding in the online event tickets marketplace. Without knowing more, however, it is unclear that the practices your question describes constitute unfair or deceptive acts or practices under Section 5 of the FTC Act. I look forward to learning more about these and other practices from the output from our Online Event Ticketing Workshop.

The Honorable Bobby L. Rush (D-IL)

1. **In 2014, the Federal Trade Commission (FTC) published a report called "Data Brokers: A Call for Transparency and Accountability" that shed light on the secretive world of data brokers that buy and sell vast amounts of consumer personal information, often entirely behind the scenes. The FTC's report called on Congress to pass legislation that would require data brokers to be more transparent and give consumers the right to opt-out, among other things.**

    a. **Do you still agree that Congress should pass legislation addressing data brokers?**

The current Commission has not taken a position on data broker legislation. It has supported data security legislation that would give the Commission authority to seek civil penalties; conduct targeted APA rulemaking; and exercise jurisdiction over common carriers and non-profit entities. I also support congressional efforts to consider federal privacy legislation. I believe it is important for the Congress to craft such legislation to address more seamlessly consumers' legitimate concerns regarding the collection, use, and sharing of their data and businesses' need for clear rules of the road, while retaining the flexibility required to foster innovation and competition. The Commission would be pleased to share our expertise in any way that Congress deems helpful to assist with formulating appropriate legislation.

2. **While innovation in the tech industry is having a tremendous impact on our economy and the lives of everyday Americans, it is also creating new challenges in protecting consumers and competitive markets. I have heard reports of certain online platforms giving their subsidiary businesses preferential treatment over their competitors.**

    a. **Are you looking into anti-consumer and anti-competitive behaviors of this nature?**

Please see the answer to question 2.b below.

    b. **In your opinion, does the FTC currently have the authority and capacity to curtail this behavior?**

The FTC does not publicly comment on pending law enforcement investigations. As a general matter, we examine carefully conduct in markets within our jurisdiction, including those involving online platforms. As more and more of the nation's commerce takes place on online platforms, the public and the antitrust agencies are devoting increasing attention to the operation of these platforms. For example, the Bureau of Competition recently announced the creation of a task force to enhance the Commission's antitrust focus on technology-related ecosystems, including technology platforms as well as markets for online advertising, social networking, mobile operating systems, and apps.

Under the U.S. antitrust laws, e-commerce firms with market power are prohibited from engaging in conduct that anticompetitively excludes rivals. Large market share alone, however,

is not a violation of the U.S. antitrust laws. Whether any particular policy of preferential access or limits on communications with customers qualifies as exclusionary is fact-driven and highly dependent on the actual market dynamics in the specific markets at issue. The Technology Task Force (TTF) will monitor competition in U.S. technology markets, investigate any conduct in these markets that may harm competition, and, when warranted, take actions to ensure that consumers benefit from free and fair competition.

On the consumer protection front, the FTC's core deception and unfairness authorities are flexible standards that have allowed the agency to protect consumers in new markets for decades; and, in many ways, online markets are no different. That said, I believe consumers would benefit if the FTC had broader enforcement authority to take action against common carriers and non-profits, which it cannot currently do under the FTC Act. Furthermore, as noted above, I do support congressional efforts to consider new legislative tools that are focused on protecting consumers in the digital economy. Such efforts should begin with agreement on the harms Congress is trying to address and work from there to appropriate remedies and authorities. Congress should further recognize the tradeoffs inherent in any such efforts, including the impacts on innovation and competition. Should Congress grant the FTC new authority, you can be assured that the agency will continue to be vigilant and that we will not hesitate to take strong and appropriate action against any act or practice that violates any statute that we enforce.

3. **As all of you know, robocalls are extremely burdensome on consumers and every effort needs to be taken to ensure that consumers are not being taken advantage of by these unscrupulous actors. I am also concerned by the reports I have heard that robocalls are now being used by online contact lens retailers to usurp the verification of contact lens prescriptions, placing consumers at an even greater risk of receiving the wrong Class II or III medical devices.**

    a. **Do you agree that efforts need to be taken to update the passive verification process?**

When Congress enacted the Fairness to Contact Lens Consumers Act ("FCLCA"), it determined that passive verification was necessary to balance the interests of prescription portability and consumer health. Congress was aware that passive verification could, in some instances, allow sellers to sell contact lenses based on an invalid or inaccurate prescription, and that this could potentially lead to health risks. In the May 28, 2019 Supplemental Notice of Proposed Rulemaking ("SNPRM"), the Commission proposed several changes to improve the passive verification process. The Commission proposed that sellers who use automated telephone verification messages would have to: (1) record the entire call and preserve the complete recording; (2) begin the call by identifying it as a prescription verification request made in accordance with the Contact Lens Rule; (3) deliver the verification message in a slow and deliberate manner and at a reasonably understandable volume; and (4) make the message repeatable at the prescriber's option. This proposal enables prescribers to fulfill their role as protectors of patients' eye health because prescribers cannot correct and police invalid, inaccurate, and expired prescriptions if they cannot comprehend a seller's verification request.

Additionally, the Commission proposed changes that would increase patients' access to their prescription, maintain patient choice and flexibility, and potentially reduce the number of

verification requests. Under the proposal, a prescriber, with the patient's verifiable affirmative consent, has the option to provide the patient with a digital copy of the prescription in lieu of a paper copy. Moreover, although the Contact Lens Rule has always required that prescribers, upon request, provide any person designated to act on behalf of the patient with a copy of the patient's valid contact lens prescription, the Rule did not prescribe a time limit in which this copy had to be provided. The Commission proposed requiring that a prescriber respond to requests for an additional copy of a prescription within forty business hours. To facilitate patients' ability to use their prescriptions, another proposed change would require sellers to provide a mechanism that would allow patients to present their prescriptions directly to sellers.

Finally, the Commission proposed amending the prohibition on seller alteration of prescriptions to address concerns about the misuse of passive verification to substitute a different brand and manufacturer of lenses. The proposal requires a seller who makes an alteration to provide a verification request to the prescriber that includes the name of a manufacturer or brand other than that specified by the patient's prescriber. There is an exception if the patient entered that manufacturer or brand on the seller's order form or the patient orally requested it from the seller.

The Commission will consider comments received in response to the SNPRM and, if appropriate, make changes before issuing a final rule.

b. Do you agree that robocalls need to be eliminated from use within the passive verification system?

An effective verification process enables prescribers, when necessary, to prevent improper sales and allows sellers to provide consumers with their prescribed contact lenses without delay. The FCLCA expressly permits telephone communication for verification and the Commission believes it would be contrary to Congressional intent to prohibit use of automated technology for the purpose of prescription verification. The Commission does not have empirical data showing the frequency of incomplete or incomprehensible automated telephone messages or that a phone call with an automated message is necessarily less reliable than one with a person. The evidence suggests that these calls can be an efficient method of verification. However, the Commission recognizes the burden on prescribers and potential health risk to patients from incomplete or incomprehensible automated telephone messages. As described in response to question 3.a, the Commission has proposed changes to automated telephone messages that would improve the verification process.

c. Could you support updating the Fairness to Contact Lens Consumers Act to eliminate robocalls and update the passive verification system to include secured emails and patient portals to verify and document contact lens prescription verification?

Under the current Rule, a "seller may sell contact lenses only in accordance with a contact lens prescription for the patient that is: (1) Presented to the seller by the patient or prescriber directly or by facsimile; or (2) Verified by direct communication." 16 C.F.R. § 315.5(a). Because the Rule's definition of direct communication already includes electronic mail, a seller and a prescriber could use email during the verification process. In the December 7, 2016 Notice of Proposed Rulemaking ("NPRM"), the Commission made an initial determination that a portal

could be used by a prescriber or a patient to "directly" present a contact lens prescription to a seller. The Commission will consider comments received in response to this initial determination and, if appropriate, make changes before issuing a final rule.

4. **In December 2016, the FTC issued a Notice of Proposed Rulemaking to update the Contact Lens Rule. As a part of this process, providers and manufacturers of contact lenses urged the FTC to require common-sense changes to the current contact lens market, including quantity limits and ways to update methods of communication under the passive verification process. The FTC responded by stating that there was insufficient evidence that consumers are buying excessive quantities of contact lenses and that it did not have the statutory authority to update the passive verification process.**

    a. **Do you support efforts to ensure patient safety regarding the current proposed rulemaking process that will include patients only receiving contact lenses as prescribed under the valid prescription?**

Federal law does not permit a seller to sell contact lenses to a patient unless the seller has obtained a copy of the prescription or the verified the patient's prescription information with the prescriber. The SNPRM's proposed changes improve patient access to contact lens prescriptions and address concerns with the passive verification requests and alterations by sellers.

5. **Last May, Rep. Michael Burgess (R-TX) and I led a letter to the FTC that laid out several concerns we have regarding the FTC rulemaking process around the Fairness to Contact Lens Consumers Act. In total, over 50 members of Congress signed this letter where we discussed the lack of enforcement action by the FTC to address the illegal sales of contact lenses and the burdensome new requirements on eye care providers.**

    a. **Has the FTC investigated or independently audited any online sellers to determine the number of lenses provided to patients?**

The Commission has not audited online sellers to determine the number of lenses provided to patients. Staff has investigated specific complaints of illegal sales related to excessive quantities. We will continue to monitor the marketplace, taking action against violations as appropriate. The Commission recently announced an enforcement action against a contact lens seller challenging the sale of contact lenses without a valid prescription. The order banned the defendant from selling contact lens and imposed a $575,000 civil penalty. *U.S. v. Duskin*, No. 1:18-cv-07359 (N.D. Cal. Dec. 6, 2018).

    b. **What enforcement mechanisms has the FTC used to ensure that sellers are not enabling the circumvention of state laws governing prescription renewal or harming patients by providing excessive numbers of contact lenses?**

In the NPRM, the Commission considered the issue of patients purchasing excessive quantities of contact lenses. Although concerned with anecdotal reports, the Commission concluded that the evidence did not show that the sale of excessive amounts of contact lenses is a widespread

problem.[1] Furthermore, a prescriber who receives a verification request for an excessive amount of lenses can contact the seller to prevent the sale from being completed.

c. How often has the FTC acted on this important safety issue?

As discussed in the response to question 5.b, the Commission does not believe that the evidence shows that excessive sale of contact lenses is a widespread problem. However, the Commission recognizes the importance of patient safety. Staff will continue to monitor the marketplace and, if appropriate, take action.

6. Many businesses are increasingly dependent on digital platforms that they do not own or operate to connect with customers.

a. With current statutory authorities in mind, what can be done to protect consumers if companies that operate these platforms offer subsidiary business products and restrict or disadvantage competitors with similar businesses on these platforms? What is the FTC doing to curtail it?

Please see the answer to question 2.b above.

b. One example of how a platform operator might harm consumers is by prohibiting businesses from communicating with their customers through that platform. Do you believe that this sort of behavior must be addressed and, if so, does the FTC currently have the statutory authority to do so?

Please see the answer to question 2.b above.

7. It has been brought to my attention that the leading internet browser has been considering a major change in what type of information is available to consumers in their product, reducing the available information that consumers use to defend themselves against a host of online threats like phishing and content spoofing.

a. As the agency charged with protecting our nation's consumers and enforcing our data privacy laws, do you have concerns about what this practice means for consumers and their data privacy and security?

Please see the answer to 7.b below.

b. Have you discussed this issue with the browsers or asked them to explain their changes and how they will impact consumer safety online? If not, do you intend to?

I understand your question to refer to how browsers display certain digital certificates in their user interface. When properly validated, digital certificates serve as proof that consumers are communicating with an authentic website and not an impostor. They also serve to encrypt traffic

[1] NPRM at 88549-50; *see also* Vision Council, U.S. Optical Market Eyewear Overview 13 (2018), https://www.ftc.gov/sites/default/files/filefield_paths/steve_kodey_ppt_presentation.pdf (noting that 82% of contact lens users had an eye exam within the last 12 months and over 95% had an exam within the last two years)

between a consumer's browser and a site's web server. In May 2018, Google announced that it would change its user interface in its Chrome browser to remove certain indicators of the presence of an expensive digital certificate – called an extended validation certificate – such as green text and a padlock icon.

I have not discussed these changes with Google. Consumers' secure online experiences depend on many factors, and the ecosystem continues to evolve quickly. I do not believe that the Commission should promote one type of certificate over another or prescribe how certificates should be displayed in user interfaces.

The Commission is nonetheless committed to promoting consumer safety online. In addition to our enforcement work, detailed in the Commission's written testimony, we engage in extensive consumer education, examples of which you may find here: https://www.consumer.ftc.gov/articles/0009-computer-security.

The Honorable Cathy McMorris Rodgers (R-WA)

1. **Commissioner Phillips, it appears that while the Commission imposes requirements that last differing lengths inside consent order-based settlements, the overall order lasts 20 years as a default. Please answer the following questions about consent orders:**

    a. **Why does the Commission, as a default, enter consent orders for 20 years?**

As a general matter, administrative orders entered in consumer protection matters sunset in 20 years, absent any intervening enforcement action. However, in certain cases, administrative orders have been shorter, for example, ten years. In contrast, federal district court orders remain in effect forever. Historically, the FTC has brought consumer protection cases against defendants permeated by unfair or deceptive practices – where there is a likelihood that the defendant will violate the order – in federal district court where the order does not sunset. In cases involving defendants less likely to violate orders – for example, companies not permeated by unfair or deceptive practices, the FTC has used the administrative process, with its shorter order-sunset period of 20 years. However, in recent years, the FTC has frequently brought cases in federal district court against companies not permeated with unfair or deceptive acts or practices. The vast majority of defendants in administrative actions continue to be companies that have violated the law but are not permeated with unfair or deceptive practices.

Administrative orders relating to anticompetitive mergers last ten years. Administrative orders relating to anticompetitive conduct, as opposed to anticompetitive mergers, last 20 years as a default, although the Commission may accept orders of shorter duration based on the facts and market realities in a given matter. And these competition conduct orders' fencing-in provisions – provisions that are broader than the unlawful conduct – typically expire well before the order sunsets.

Any party under administrative order may petition the Commission to modify or set aside the order due to changes in law or fact or to a determination that the public interest so requires, which happens from time to time.

    b. **Is there any data to support the 20-year length of consent orders?**

For consumer protection matters, there is no publicly available aggregated data to support the 20-year length of administrative consent orders. Because many of the FTC's consumer protection administrative orders involve technology companies and other rapidly evolving businesses, I believe it would be useful to examine whether 20 years is the appropriate length for an administrative order.

For competition matters, please see the answer to 1.c. below.

    c. **Are there compelling reasons for consent orders in the competition space to last longer than consumer protection cases?**

I support shortening the default duration of competition conduct orders to ten years. Since the mid-1990s, the Commission has issued over 100 competition orders. Yet, in that same period, the Commission brought enforcement actions in only three competition conduct matters more than ten years after issuing the order. In other words, limiting orders to ten years would have affected only three competition actions over the past 20 years. Furthermore, a ten-year order term would reduce the burden on companies under order, free up Commission resources, and provide greater consistency by aligning the Commission's competition conduct orders with those of the Department of Justice's Antitrust Division.

i. If so, what are those reasons?

Please see the answer to question 1.c above.

d. Has the Commission conducted a study of similar enforcement regimes and the length of consent orders issued by those other agencies and considered adjusting the FTC's standard 20-year consent order timeframe?

i. If yes, which agencies?

ii. If no, why not?

I am not aware of such a study. Twenty years is a long time, in particular in markets that develop quickly, such as those characterized by technological innovation. I support efforts to adjust the default length of our consent orders, and believe we should take seriously requests to adjust those defaults in particular cases.

2. Commissioner Phillips, I understand the desire to give the Commission more tools to hold bad actors accountable on first offenses, but I also am concerned with potentially eroding due process protections. If Congress grants the Commission first offense civil penalty authority for violations of Section 5 of the FTC Act, do you believe we should also consider an expedited track to judicial review?

I am not in favor of civil penalty authority for violations of Section 5 of the FTC Act in the first instance. The FTC's statutory jurisdiction is very broad. Not only does the agency have jurisdiction over a wide swath of the American economy, the agency has the authority to challenge conduct falling under Section 5's expansive mandate: prohibiting unfair or deceptive acts or practices. Prior to an FTC enforcement investigation, it might be difficult for some companies to recognize that their conduct is prohibited by these standards.

This broad statutory regime is balanced by the fact that the FTC does not have the authority to impose civil penalties in the first instance for violations of Section 5 of the FTC Act. This addresses the due process concerns that apply when engaging in enforcement for conduct that was not clearly proscribed. In those cases where the FTC does impose penalties for first-time

violations, clear rules – either from Congress itself or through Magnusson-Moss or APA rulemaking – should predicate the imposition of penalties.

Should new legislation include penalties for first-time violations under similarly broad standards as are currently in Section 5, expedited review may help alleviate some of the burden; but it would not address the core issue of imposing penalties where the illegality of the conduct could not readily have been anticipated.

a. Are there any other considerations we should contemplate to ensure persons' due process rights are protected under any new federal privacy regime?

In addition to the due process considerations noted above, I am concerned that excessive penalties could deter companies from exploring innovative and consumer-friendly products and services; the risk may simply be too great. This is of particular concern given that many privacy harms being contemplated result in little to no tangible consumer harm. To account for this, any penalty scheme set by Congress should balance a range of factors, including consumer harm, and be set on a graduated scale, so as to tether them to coherent set of principles set out by Congress. Furthermore, even if Congress is to impose penalties for initial violations, that scheme need not apply to every violation. Some conduct, and particularly conduct whose legality is more difficult to determine in the abstract and whose deterrence may have negative consequences, should continue to be enforced under our current structure.

3. Commissioner Phillips, I have concerns with companies making promises that potentially oversell technical capabilities or features. For example, one tech firm has advertised that what happens on your device stays on your device. But this same company allows consumers to download apps that collect consumer information and share that information with third parties. In other cases, some firms have started marketing "unhackable" devices when we know perfect security is aspirational. With respect to this concern, please answer the following:

a. Does the FTC have any existing authority to address this concern? If so, please identify such authority.

Advertising plays a critical role in our economy, providing consumers with valuable information. However, to be useful, advertising must not be misleading. The FTC Act prohibits deceptive and unfair acts or practices. The examples of advertising and product claims that you describe are troubling and could constitute deceptive or unfair practices depending upon the facts of the case. To establish that an advertisement is deceptive requires a showing that (1) there was a representation or omission, (2) the representation or omission was likely to mislead consumers acting reasonably under the circumstances, and (3) the representation or omission was material.[2] To establish that a practice is unfair requires a showing that an act or practice is likely to cause

[2] *See* Federal Trade Commission Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).

substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition.[3]

b. Could the Commission's deception authority apply to these types of claims?

Yes, please see the answer to 3.a.

4. Commissioner Phillips, do you believe a private right of action, delegating enforcement authority of any new federal privacy bill to private sector plaintiffs' attorneys, will disproportionately hurt small business?

Yes.

a. If yes, please explain why.

A private right of action will have a substantial and unwarranted negative impact, particularly on small, innovative, businesses, deterring them from innovating and growing jobs, as they prioritize lawsuit avoidance over doing what they do best.

Data collection and use are endemic to our economy and are the engines of significant economic growth and consumer benefit. Any federal privacy bill will thus apply to a vast array of companies, large and small.

No matter the size of the firm, the strike suit behavior encouraged by a private right of action threatens economic vitality. Businesses will settle cases for substantial sums, even where the cases lack merit or where consumer injury is limited. This is particularly a concern for smaller companies, as their limited staffs and natural start-up mistakes in a complex regulatory environment may make them a specific target for the private bar, while they have fewer resources to avoid and challenge such suits than their larger competitors. As a consequence, entrepreneurs may avoid making decisions and offering new services that enhance innovation and competition. They will pay nuisance amounts in settlement, mis-allocating resources. Recent FTC experience bears this out. Patent rights are critical to encouraging innovation. But they can be abused, as they were in the notorious MPHJ scheme, where many small businesses were threatened with patent litigation and paid substantial sums.[4] Federal enforcement avoids risks like these by removing the economic incentives of lawyers from the calculus.

A new federal privacy law must provide for rules and regulation, but it should do so in a way that best permits for future growth and innovation and that encourages investment and risk-taking.

---

[3] Federal Trade Commission Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

[4] *See, e.g.*, FTC Approves Final Order Barring Patent Assertion Entity From Using Deceptive Tactics, Mar. 17, 2015, https://www.ftc.gov/news-events/press-releases/2015/03/ftc-approves-final-order-barring-patent-assertion-entity-using (discussing FTC administrative consent with MPHJ Technology Investments, LLC, where small businesses were targeted with demand letters). *See also* FTC Staff Report, *Patent Assertion Activity: An FTC Study*, Oct. 2016, https://www.ftc.gov/reports/patent-assertion-entity-activity-ftc-study (examining non-public information and data covering the period 2009 to 2014 from 22 PAEs, 327 PAE affiliates, and more than 2100 holding entities obtained through compulsory process orders using the FTC's Section 6(b) authority).

Government enforcement of a privacy law, rather private lawsuits, is the best way to balance those interests.

5. **Commissioner Phillips, can you explain how a fragmented internet, regulated on a state-by-state basis, may result in different online opportunities, options, and experiences for people in rural communities than people in urban areas?**

Application of a single legal framework across the country provides consistency and fairness, which is especially important to the businesses that operate in many rural communities. Allowing different states to apply different laws – laws whose content we do not and cannot yet know – could result in radically different regimes in different states, and, accordingly, radically different goods and services offered by technology companies. It will favor large, national, firms; and disproportionately hurt smaller operators, many of which may be local. In some cases, technology companies may choose not to provide certain services to citizens of some states due to the undue legal and financial risks a particular state's laws would impose. A single federal law could help avoid such outcomes and ensure that consumers across the country are treated fairly and equally.

6. **Commissioner Phillips, how difficult would it be for the FTC to enforce a federal privacy law with various, potentially competing, state laws also in effect?**

Where we have a variety of differing state laws, the FTC will have to engage in competing investigations and lawsuits with state law enforcement agencies, rather than more efficient collaborations. The result will be less federal-state cooperation and more protracted investigations, more complicated litigation, and more challenging settlement environments. We may also face situations where similar – yet distinct – laws are subject to different legal interpretations by courts, removing some of the Commission's power to help shape consistency in that interpretation through our own case selection and legal arguments in federal court.

7. **Commissioner Phillips, is there an impact we should be considering when crafting privacy legislation that could have an unintended or negative impact on competition in the U.S. marketplace? What factors should be considered to guard against these unintended consequences?**

Privacy legislation will involve tradeoffs, in particular when it comes to innovation and competition. Large companies can more easily bear the costs of compliance, while smaller entities will face more risk and uncertainty. That means that legislation carries the possibility of entrenching incumbents while limiting new market entrants who may provide competition and innovative, valuable products and services. This is an issue that I have spoken about before,[5] and there is already some evidence that since the implementation of GDPR, investment in startups is

[5] Commissioner Noah Joshua Phillips, *Keep It: Maintaining Competition in the Privacy Debate*, Internet Governance Forum USA, Washington, DC (July 27, 2018), https://www.ftc.gov/public-statements/2018/07/keep-it-maintaining-competition-privacy-debate.

down in Europe[6] and more market share is flowing to the largest companies.[7] Time will tell about that impact.

To guard against these concerns, as Congress moves forward to regulate so much of the economy, it should take care and be cognizant about the impacts and tradeoffs. This means moving more cautiously and learning from the experiences of jurisdictions that have already instituted new privacy rules. Congress should also favor simplicity over complexity, especially in the early days, with lower penalties and federal preemption to create a single set of rules of the road for businesses and consumers.

8. **Commissioner Phillips, this year a number of state legislatures are considering laws requiring proprietary auto Dealer Management Systems (DMS) to be accessed by unlicensed, unmonitored third parties. There are questions about the cybersecurity and privacy risks raised in these circumstances even with well-intended goals for example in Arizona and Montana. Are you aware of these state laws and do they raise on cybersecurity or privacy concerns?**

I have not studied those laws in depth, and they are outside the jurisdiction of the Commission's authority. Laws mandating the sharing of data can raise competition concerns, as well as cybersecurity and privacy ones. All these, and open-access, are important goals that must be managed.

9. **Commissioner Phillips, my understanding is when the FTC seeks to recover ill-gotten gains from an entity that has violated FTC competition rules, the Commission only seeks to disgorge the profit from that unlawful act. Is that correct?**

Yes, in competition cases, the equitable relief available to the FTC includes disgorgement of the improperly obtained gains.

   a. **Please explain how the Commission calculates the profit of those ill-gotten gains.**

The Commission estimates, based on the available facts and data, how much profit the defendant(s) would have earned absent the anticompetitive conduct. The estimation process is heavily influenced by the facts of the particular case and may require sophisticated modeling. Therefore, the Bureau of Competition works closely with the Bureau of Economics and with the FTC's experts on the specific matter to estimate the appropriate disgorgement amount. At trial, the FTC bears the burden of persuading the court that it has a reasonable basis for the amount of monetary relief sought.

---

[6] Jian Jia, Ginger Jin & Liad Wagman, *The short-run effects of GDPR on technology venture investment*, VOX EU (Jan. 7, 2019), https://voxeu.org/article/short-run-effects-gdpr-technology-venture-investment.
[7] Björn Greif, *Study: Google is the biggest beneficiary of the GDPR*, CLIQZ (Oct. 10, 2018), https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr.

For example, in *AbbVie*, the FTC sued several pharmaceutical companies for filing sham patent infringement lawsuits to delay entry of generic AndroGel. The FTC's testifying economic expert determined that, absent the sham litigation, generic AndroGel products would have entered market in 2012. He then estimated that, as a result of delaying generic competition, defendants earned about $1 billion more than they otherwise would have between 2012 and 2018. The judge agreed with the overall approach taken by the FTC's expert but reduced $450 million based on his findings that generic entry would have happened one year later than the FTC claimed and that the generic products had fully penetrated the market by 2017 and thus no part of the defendants' profit after that point resulted from the anticompetitive conduct.

The Honorable Robert E. Latta (R-OH)

1. **Commissioner Phillips, we want companies of all sizes to protect consumer information, but we do not want new privacy obligations to crush small businesses and benefit big companies. In the 2012 FTC privacy report, the Commission grappled with this specific concern and excluded some small businesses from its recommendations.**

    a. **How do you think we should be addressing this concern?**

As a general matter, the best rules are those that can be applied to firms of all sizes. To the extent Congress is considering excluding small businesses from privacy legislation, we would suggest focusing not on the size of the company, but on the amount and sensitivity of the data the company collects. A company with few employees can collect highly-sensitive data of millions of consumers, and such a company should be subject to privacy rules. As you note, this is the approach we took in the 2012 Privacy Report.

The Honorable Michael C. Burgess (R-TX)

1. **Commissioner Phillips, we know that small businesses have suffered in Europe since the implementation of the General Data Protection Regulation (GDPR). In fact, according to some reports, investments in startups are down an astounding 40 percent.**

    a. **How can we guard against the same happening here?**

Because the GDPR has now been in effect for only a year, there is a limited basis upon which researchers and others have been able to draw conclusions about potential effects that the GDPR has had on investments in startups. That said, the FTC's recent Hearings on Competition and Consumer Protection in the 21st Century did include discussion of research showing that, in the European Union, the number of venture capital technology deals and the average amount invested per deal declined in the first several months after the GDPR took effect. Researchers have stated their intent to monitor to see whether those observations remain true on a longer-term basis. The FTC will keep abreast of such research.

Small firms want growth and ease of access to markets. They want to focus on building their businesses, not legal compliance. Congress recognized this dynamic with respect to the securities laws when it passed the JOBS Act in 2012. The best way to protect startups in a new privacy law are to keep the rules clear and constant over time (including limiting rulemaking authority), preempt a multiplicity of state laws, and ensure that enforcement does not chill innovation.

2. **Commissioner Phillips, when the FTC enjoyed broad rulemaking authority in the 1970s it got so bad that a Democratic-led Congress cut funding to the Commission for several days.**

    a. **How should the events of the past inform our discussion about FTC rulemaking today and under future administrations**

Congress has the legal and political mandate to make the key decisions about what the rules of the road for business and the public should be. When too much rulemaking authority is delegated, regulators may usurp legislative authority and the public may end up with rules the content of which can change dramatically over short periods of time. Businesses need confidence to plan and consumers are best off when they can rely on rules they know. Too much delegated power also is not good for the Commission itself, involving the agency – a law enforcement body – and its Commissioners in political issues, distracting us from our attention on our core, bipartisan mission.

    b. **Do you have any concerns about the scope of the Administrative Procedures Act rulemaking in conjunction with privacy legislation? If so, what are those concerns?**

The purported benefit of APA-style rulemaking is its efficiency, but that can be a bad thing depending on the scope of the authority. Privacy legislation necessarily demands complex value judgments, as it must define harms, create new rights for American consumers that have not previously existed in law, and impose substantial new obligations on American businesses. These are weighty issues that are the domain of our democratically elected Congress, not agency Staff and Commissioners. To the extent the Commission has rulemaking authority under any new privacy legislation, that rulemaking should be limited and targeted. It should not involve establishing substantive standards, but rather focus on the technical details – such as the form of a particular notice – and be subject to the very clear guidance of Congress to ensure that the agency remains faithful to Congressional intent.

Additional Questions for the Record

Subcommittee on Consumer Protection and Commerce
Hearing on
"Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security"
May 8, 2019

The Honorable Rohit Chopra, Commissioner
The Federal Trade Commission

The Honorable Jan Schakowsky (D-IL)

1. **On June 11, 2019, the Federal Trade Commission (FTC) will hold a workshop on online event tickets. I have heard reports of a number of consumer protection issues concerning online event tickets that raise serious concerns and I hope the FTC will consider addressing these issues during its workshop. For example, I have heard concerns that primary ticket platforms have begun forcing purchasers to disclose personally identifiable information by creating an account with the primary ticket seller to use a ticket, even when tickets are resold on a secondary market. I have also heard complaints about primary ticket sellers that hold tickets back from the market pursuant to agreements with venues, artists, or other partners. In addition, I have received complaints about primary ticket vendors putting technological restrictions on the transfer of tickets, which can prevent ticket holders from reselling or giving away tickets if they cannot attend the event.**

    a. **Will the FTC examine these issues at its upcoming hearing on online event tickets?**

These are critical issues. In addition to exploring these issues at the workshop, we invited public comments on this marketplace to inform our approach going forward.

    b. **Has the FTC received similar complaints from consumers?**

The most common consumer complaints we receive about online event ticketing concern hidden or inadequately disclosed ticketing fees in the primary and secondary markets, and consumers who report ticket resellers misled them to believe they were purchasing tickets from the venue or authorized seller at face value (when in fact they were purchasing tickets from resellers at a significant markup). The Commission also received several thousand consumer comments in connection with the upcoming ticketing workshop. Those comments overwhelmingly concerned hidden or inadequately disclosed ticketing fees and/or the high cost of such fees. While the FTC may also have received consumer complaints or comments regarding the practices you outline, they do not appear to be as prevalent.

c. Do you agree that, if true, these practices raise concerns about unfair or deceptive practices in the market for online event tickets?

Yes. In addition, the ticketing market is highly concentrated and vertically integrated with other parts of the industry that can impact ticket practices and prices. It's concerning that one company controls so many aspects of the entertainment industry – from ticketing, to live venues, to resale technologies. It can be much easier for firms to engage in practices that are harmful to consumers when they face little competition. Other problems arise when a company is able to use their dominance in one market to choke off competition in ancillary markets. The FTC should pay close attention for potential anticompetitive practices in this industry and bring enforcement actions when appropriate.

The Honorable Bobby L. Rush (D-IL)

1. **In 2014, the Federal Trade Commission (FTC) published a report called "Data Brokers: A Call for Transparency and Accountability" that shed light on the secretive world of data brokers that buy and sell vast amounts of consumer personal information, often entirely behind the scenes. The FTC's report called on Congress to pass legislation that would require data brokers to be more transparent and give consumers the right to opt-out, among other things.**

    a. **Do you still agree that Congress should pass legislation addressing data brokers?**

Yes, I agree.

2. **While innovation in the tech industry is having a tremendous impact on our economy and the lives of everyday Americans, it is also creating new challenges in protecting consumers and competitive markets. I have heard reports of certain online platforms giving their subsidiary businesses preferential treatment over their competitors.**

    a. **Are you looking into anti-consumer and anti-competitive behaviors of this nature?**

    b. **In your opinion, does the FTC currently have the authority and capacity to curtail this behavior?**

The Commission already has a robust set of tools for tackling these challenges, and it is essential we use them not only against small players but also against large firms that pose risks to consumers and competition. I have previously advocated that the Commission should use its competition rulemaking authority to help rein in anticompetitive practices; potential abuses by online dominant tech platforms is one area where the Commission's competition rulemaking authority may be useful. In addition, the Commission has the authority to study industries and collect industry-wide data through our Section 6(b) authority. The Commission should use this authority to study the business practices of online platforms, which will help fine tune potential future law enforcement actions.

Under the U.S. antitrust laws, firms with market power are prohibited from engaging in conduct that anticompetitively excludes rivals or maintains a monopoly, as well as conduct that amounts to attempted monopolization. The "unfair method of competition" prong of the FTC Act's Section 5 also prohibits conduct that violate the policies that underlie the antitrust laws, or conduct that constitutes incipient violations of those laws.

Unilateral conduct by tech firms that meet any of these criteria is especially dangerous to our economy, because of the loss in innovation by excluded nascent competitors. Some of the best innovations in our economy have traditionally been by small firms who, in today's economy, may be at risk of exclusion by powerful online platforms. The vast data troves and network

effects of large online platforms may create insurmountable entry barriers for nascent competitors, which in turn would give online platforms durable market power.

3. **As all of you know, robocalls are extremely burdensome on consumers and every effort needs to be taken to ensure that consumers are not being taken advantage of by these unscrupulous actors. I am also concerned by the reports I have heard that robocalls are now being used by online contact lens retailers to usurp the verification of contact lens prescriptions, placing consumers at an even greater risk of receiving the wrong Class II or III medical devices.**

    a. **Do you agree that efforts need to be taken to update the passive verification process?**

When Congress enacted the Fairness to Contact Lens Consumers Act ("FCLCA"), it determined that passive verification was necessary to balance the interests of prescription portability and consumer health. Congress was aware that passive verification could, in some instances, allow sellers to sell contact lenses based on an invalid or inaccurate prescription, and that this could potentially lead to health risks. In the May 28, 2019 Supplemental Notice of Proposed Rulemaking ("SNPRM"), the Commission proposed several changes to improve the passive verification process. The Commission proposed that sellers who use automated telephone verification messages would have to: (1) record the entire call and preserve the complete recording; (2) begin the call by identifying it as a prescription verification request made in accordance with the Contact Lens Rule; (3) deliver the verification message in a slow and deliberate manner and at a reasonably understandable volume; and (4) make the message repeatable at the prescriber's option. This proposal enables prescribers to fulfill their role as protectors of patients' eye health because prescribers cannot correct and police invalid, inaccurate, and expired prescriptions if they cannot comprehend a seller's verification request.

Additionally, the Commission proposed changes that would increase patients' access to their prescription, maintain patient choice and flexibility, and potentially reduce the number of verification requests. Under the proposal, a prescriber, with the patient's verifiable affirmative consent, has the option to provide the patient with a digital copy of the prescription in lieu of a paper copy. Moreover, although the Rule has always required that prescribers, upon request, provide any person designated to act on behalf of the patient with a copy of the patient's valid contact lens prescription, the Rule did not prescribe a time limit in which this copy had to be provided. The Commission proposed requiring that a prescriber respond to requests for an additional copy of a prescription within forty business hours. To facilitate patients' ability to use their prescriptions, another proposed change would require sellers to provide a mechanism that would allow patients to present their prescriptions directly to sellers.

Finally, the Commission proposed amending the prohibition on seller alteration of prescriptions to address concerns about the misuse of passive verification to substitute a different brand and manufacturer of lenses. The proposal requires a seller who makes an alteration to provide a verification request to the prescriber that includes the name of a manufacturer or brand other than that specified by the patient's prescriber. There is an exception if the patient entered that manufacturer or brand on the seller's order form or the patient orally requested it from the seller.

The Commission will consider comments received in response to the SNPRM and, if appropriate, make changes before issuing a final rule.

b. Do you agree that robocalls need to be eliminated from use within the passive verification system?

An effective verification process enables prescribers, when necessary, to prevent improper sales and allows sellers to provide consumers with their prescribed contact lenses without delay. The FCLCA expressly permits telephone communication for verification and the Commission believes it would be contrary to Congressional intent to prohibit use of automated technology for the purpose of prescription verification. The Commission does not have empirical data showing the frequency of incomplete or incomprehensible automated telephone messages or that a phone call with an automated message is necessarily less reliable than one with a live person. The evidence suggests that these calls can be an efficient method of verification. However, the Commission recognizes the burden on prescribers and potential health risk to patients from incomplete or incomprehensible automated telephone messages. As described in response to question 3.a, the Commission has proposed changes to automated telephone messages that would improve the verification process.

c. Could you support updating the Fairness to Contact Lens Consumers Act to eliminate robocalls and update the passive verification system to include secured emails and patient portals to verify and document contact lens prescription verification?

Under the current Rule, a "seller may sell contact lenses only in accordance with a contact lens prescription for the patient that is: (1) Presented to the seller by the patient or prescriber directly or by facsimile; or (2) Verified by direct communication." 16 C.F.R. § 315.5(a). Because the Rule's definition of direct communication already includes electronic mail, a seller and a prescriber could use email during the verification process. In the December 7, 2016 Notice of Proposed Rulemaking ("NPRM"), the Commission made an initial determination that a portal could be used by a prescriber or a patient to "directly" present a contact lens prescription to a seller. The Commission will consider comments received in response to this initial determination and, if appropriate, make changes before issuing a final rule.

4. **In December 2016, the FTC issued a Notice of Proposed Rulemaking to update the Contact Lens Rule. As a part of this process, providers and manufacturers of contact lenses urged the FTC to require common-sense changes to the current contact lens market, including quantity limits and ways to update methods of communication under the passive verification process. The FTC responded by stating that there was insufficient evidence that consumers are buying excessive quantities of contact lenses and that it did not have the statutory authority to update the passive verification process.**

a. **Do you support efforts to ensure patient safety regarding the current proposed rulemaking process that will include patients only receiving contact lenses as prescribed under the valid prescription?**

The Commission does not believe patients should be able to purchase contacts without a valid prescription. The SNPRM's proposed changes improve patient access to contact lens prescriptions and address concerns with the passive verification requests and alterations by sellers.

5. **Last May, Rep. Michael Burgess (R-TX) and I led a letter to the FTC that laid out several concerns we have regarding the FTC rulemaking process around the Fairness to Contact Lens Consumers Act. In total, over 50 members of Congress signed this letter where we discussed the lack of enforcement action by the FTC to address the illegal sales of contact lenses and the burdensome new requirements on eye care providers.**

   a. **Has the FTC investigated or independently audited any online sellers to determine the number of lenses provided to patients?**

No.

   b. **What enforcement mechanisms has the FTC used to ensure that sellers are not enabling the circumvention of state laws governing prescription renewal or harming patients by providing excessive numbers of contact lenses?**

In the NPRM, the Commission considered the issue of patients purchasing excessive quantities of contact lenses. Although concerned with anecdotal reports, the Commission concluded that the evidence did not show that the sale of excessive amounts of contact lenses is a widespread problem[1]. Furthermore, a prescriber who receives a verification request for an excessive amount of lenses can contact the seller to prevent the sale from being completed. Staff has investigated specific complaints of illegal sales related to excessive quantities. We will continue to monitor the marketplace, taking action against violations as appropriate.

   c. **How often has the FTC acted on this important safety issue?**

As discussed in the response to question 5.b, the Commission does not believe that the evidence shows that excessive sale of contact lenses is a widespread problem. However, the Commission recognizes the importance of patient safety. Staff will continue to monitor the marketplace and, if appropriate, take action.

6. **Many businesses are increasingly dependent on digital platforms that they do not own or operate to connect with customers.**

---

[1] NPRM at 88549-50; *see also* Vision Council, U.S. Optical Market Eyewear Overview 13 (2018), https://www.ftc.gov/sites/default/files/filefield_paths/steve_kodey_ppt_presentation.pdf (noting that 82% of contact lens users had an eye exam within the last 12 months and over 95% had an exam within the last two years)

a. **With current statutory authorities in mind, what can be done to protect consumers if companies that operate these platforms offer subsidiary business products and restrict or disadvantage competitors with similar businesses on these platforms? What is the FTC doing to curtail it?**

b. **One example of how a platform operator might harm consumers is by prohibiting businesses from communicating with their customers through that platform. Do you believe that this sort of behavior must be addressed and, if so, does the FTC currently have the statutory authority to do so?**

Please see the answer to question 2.

7. **It has been brought to my attention that the leading internet browser has been considering a major change in what type of information is available to consumers in their product, reducing the available information that consumers use to defend themselves against a host of online threats like phishing and content spoofing.**

   a. **As the agency charged with protecting our nation's consumers and enforcing our data privacy laws, do you have concerns about what this practice means for consumers and their data privacy and security?**

   b. **Have you discussed this issue with the browsers or asked them to explain their changes and how they will impact consumer safety online? If not, do you intend to?**

I understand your question to refer to how browsers display certain digital certificates in their user interface. In May 2018, Google announced that it would change its user interface in its Chrome browser to remove certain indicators of the presence of an expensive digital certificate – called an extended validation certificate – such as green text and a padlock icon.

I have not discussed these changes with Google. Consumers' secure online experiences depend on many factors, and the ecosystem continues to evolve quickly. I do not believe that the Commission should promote one type of certificate over another or prescribe how certificates should be displayed in user interfaces.

○