AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PROTECTING CUSTOMER NETWORK PROPRIETARY INFORMATION IN THE INTERNET AGE

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JULY 11, 2018

Serial No. 115–148

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
35–164 WASHINGTON : 2019

COMMITTEE ON ENERGY AND COMMERCE

GREG WALDEN, Oregon
Chairman

JOE BARTON, Texas
Vice Chairman
FRED UPTON, Michigan
JOHN SHIMKUS, Illinois
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
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
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota
TIM WALBERG, Michigan
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina

FRANK PALLONE, JR., New Jersey
Ranking Member
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
MICHAEL F. DOYLE, Pennsylvania
JANICE D. 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
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

MARSHA BLACKBURN, Tennessee
Chairman

LEONARD LANCE, New Jersey
Vice Chairman
JOHN SHIMKUS, Illinois
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
BILL FLORES, Texas
SUSAN W. BROOKS, Tennessee
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
GREG WALDEN, Oregon *(ex officio)*

MICHAEL F. DOYLE, Pennsylvania
Ranking Member
PETER WELCH, Vermont
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
RAUL RUIZ, California
DEBBIE DINGELL, Michigan
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
JERRY MCNERNEY, California
FRANK PALLONE, JR., New Jersey *(ex officio)*

CONTENTS

	Page
Hon. Marsha Blackburn, a Representative in Congress from the State of Tennessee, opening statement	1
Prepared statement	3
Hon. Leonard Lance, a Representative in Congress from the State of New Jersey, prepared statement	4
Hon. Michael F. Doyle, a Representative in Congress from the Commonwealth of Pennsylvania, opening statement	4
Prepared statement	6
Hon. Anna G. Eshoo, a Representative in Congress from the State of California, opening statement	7
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, prepared statement	8
Hon. Greg Walden, a Representative in Congress from the State of Oregon, prepared statement	79

WITNESSES

Hance Haney, Director and Senior Fellow, Technology and Democracy Project, Discovery Institute	9
Prepared statement	12
Robert McDowell, Senior Fellow, Hudson Institute, Former Commissioner, Federal Communications Commission	23
Prepared statement	25
Laura Moy, Deputy Director, Georgetown Law Center on Privacy and Technology	33
Prepared statement	35

SUBMITTED MATERIAL

Article entitled, "Smart TVs are watching us now," Axios, July 5, 2018	81
Article entitled, "How—and why—Apple, Google, and Facebook Follow you Around in Real Life," Fast Company, December 22, 2017	83
Article entitled, "Facebook scraped call, text message data for years from Android phones," Ars Technica, March 24, 2018	87

PROTECTING CUSTOMER NETWORK PROPRIETARY INFORMATION IN THE INTERNET AGE

WEDNESDAY, JULY 11, 2018

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:13 a.m., in room 2322, Rayburn House Office Building, Hon. Marsha Blackburn (chairman of the subcommittee) presiding.

Present: Representatives Blackburn, Lance, Shimkus, Latta, Guthrie, Olson, Johnson, Long, Flores, Brooks, Collins, Walters, Costello, Doyle, Welch, Clarke, Ruiz, Dingell, Eshoo, Engel, Butterfield, Matsui, McNerney, and Pallone (ex officio).

Staff Present: Jon Adame, Policy Coordinator, Communications and Technology; Kristine Fargotstein, Detailee, Communications and Technology; Sean Farrell, Professional Staff Member, Communications and Technology; Adam Fromm; Director of Outreach and Coalitions; Elena Hernandez, Press Secretary; Tim Kurth, Deputy Chief Counsel, Communications and Technology; Lauren McCarty, Counsel, Communications and Technology; Drew McDowell, Executive Assistant; Evan Viau, Legislative Clerk, Communications and Technology; Jeff Carroll, Minority Staff Director; Jennifer Epperson, Minority FCC Detailee; Tiffany Guarascio, Minority Deputy Staff Director and Chief Health Advisor; Alex Hoehn-Saric, Minority Chief Counsel, Communications and Technology; Jerry Leverich, Minority Counsel; Dan Miller, Minority Policy Analyst; and C.J. Young, Minority Press Secretary.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Mrs. BLACKBURN. The Subcommittee on Comms and Tech will now come to order. And the chair now recognizes herself for 5 minutes for an opening statement.

Good morning to everyone. And welcome to today's hearing on protecting consumer privacy. And if you have not done so, I would encourage you to get your acronym app out as you try to follow along with what we have before us today.

This is a topic that has attracted attention in a variety of contexts, and one that I am so pleased that we are discussing today. And I want to say thank you to our witnesses who are sharing

their expertise with us as we strive to protect customer privacy when communicating in the internet age.

Over 20 years ago, Congress realized the importance of protecting the confidentiality of Customer Proprietary Network Information, CPNI, when consumers use their primary method for instantaneous communication, which at that point was telephone calls.

The rules that the FCC initially adopted to implement the statutory CPNI requirements only covered information from traditional call records. But over time, these protections have evolved to cover new forms of communication like interconnected Voice over IP, or VoIP, calls, and even information collected by telecommunications carriers on mobile devices.

By enacting section 222, Congress established a specific statutory structure that acknowledged that consumers share sensitive data when they communicate over the phone. This was based on the assumption that only the telecommunications carrier had access to that data. In the internet age, telecommunications laws have been disrupted just like everything else. In some cases, app developers operating systems and Edge providers have access to the same exact CPNI that telecom carriers are required to protect in various ways.

Consumers now use these different forms of communication interchangeably to serve the same purpose. For example, if a consumer uses his or her mobile phone to call someone using the standard telephone function on their cell phone, that call is traveling over the public switch telecom network and would be protected by the current CPNI rules and enforced by the FCC. If that same consumer uses the exact same cell phone to call the exact same person but uses a voice-based app to place a call, the communication would not be going over the PSTN and not be protected by the CPNI rules.

As I said, you need your acronym app for this one.

Both calls are conveying the same information, but the consumer's information in the second scenario is not protected in the same manner as the first scenario. This leads to a problem where consumers do not have the same privacy protections when using the same device for essentially the same purpose.

This is when the FCC's 2016 Privacy Order was a consumer protection vehicle that drove at the wrong target. The Commission's inability to locate all the other traffic out there is precisely when wheels came off.

As I have suggested before, the solution to this problem is broad privacy legislation, which is why I introduced legislation on the subject almost a year ago that steers us in the right direction. The BROWSER Act is comprehensive bipartisan privacy legislation that will give Americans seamless protection across all of their electronic communications.

As we discuss these important issues today, we need to consider innovation and consumer privacy needs across the entire internet ecosystem so we can arrive at a solution that works for everyone.

At this time, I yield the remainder of my time to Mr. Lance for his opening.

[The prepared statement of Mrs. Blackburn follows:]

PREPARED STATEMENT OF HON. MARSHA BLACKBURN

Good morning and welcome to today's hearing on protecting consumer privacy. This is a topic that has attracted attention in a variety of contexts, and one that I am glad to discuss today. Thank you to our witnesses for sharing your expertise with us today as we strive to protect customer privacy when communicating in the Internet age.

Over 20 years ago, Congress realized the importance of protecting the confidentiality of customer proprietary network information, or CPNI, when consumers used the primary method for instantaneous communication: telephone calls. The rules that the FCC initially adopted to implement the statutory CPNI requirements only covered information from traditional call records, but over time, these protections have evolved to cover new forms of communication-like interconnected voice over IP (VoIP) calls and even information collected by telecommunications carriers on mobile devices.

By enacting Section 222, Congress established a specific statutory structure that acknowledged that consumers share sensitive data when they communicate over the phone. This was based on the assumption that only the telecommunications carrier had access to that data. In the Internet age, telecommunications laws have been disrupted just like everything else. In some cases, app developers, operating systems, and edge providers have access to the same exact CPNI that telecommunications carriers are required to protect in various ways. Consumers now use these different forms of communication interchangeably to serve the same purpose.

For example, if a consumer uses his or her mobile phone to call someone using the standard telephone function on their cell phone, that call is traveling over the public switched telecommunications network and would be protected by the current CPNI rules, and enforced by the FCC. If that same consumer uses the exact same cell phone to call the exact same person, but uses a voice-based app to place the call, the communication would not be going over the PSTN and not be protected by the CPNI rules. Both calls are conveying the same information, but the consumer's information in the second scenario is not protected in the same manner as in the first scenario.

This leads to a problem where consumers do not have the same privacy protections when using the same device for essentially the same purpose. This is why the FCC's 2016 privacy order was a consumer protection vehicle that drove at the wrong target. The commission's inability to locate all the other traffic out there is precisely why the wheels came off it. As I have suggested before, the solution to this problem is broad privacy legislation, which is why I introduced legislation on this subject almost a year ago that steers us in the right direction—the BROWSER Act is a comprehensive, bipartisan privacy bill that will give Americans seamless protection across all their electronic communications.

As we discuss these important issues today, we need to consider innovation and consumer privacy needs across the entire Internet ecosystem so we can arrive at a solution that works for everyone.

At this time, I will yield to the remainder of my time to Mr. Lance for an opening statement.

Mr. LANCE. Thank you, Chairman Blackburn. And welcome to our distinguished panel.

Section 222 of the Communications Act was enacted during the Act's last major update in 1996. The section mandates the telecommunication entities protect consumer privacy information, as the chairman has said, CPNI.

Since 1996, the internet has revolutionized communications in so many ways. However, as breaches of consumer data repeatedly confront us, we must ensure the rules and regulations protecting consumer information are up to date and applied equally across the internet ecosystem.

The FCC has tried to keep up with the technological innovations over the past 20 years, but an outdated statute limits its efforts. It is crucial we protect consumers' sensitive information, no matter the means of communication, and without hampering innovation.

I look forward to discussing how we can update the law to conform to the challenges and opportunities of the digital age. And I yield back.

[The prepared statement of Mr. Lance follows:]

PREPARED STATEMENT OF HON. LEONARD LANCE

Thank you Chairman Blackburn and welcome to our distinguished panel.

Section 222 of the Communications Act was enacted during the Act's last major update in 1996. This section mandates that telecommunications carried protect customer proprietary network information or CPNI. Since 1996, the internet has revolutionized communications. Through innovations from Voice over IP, to apps like Snapchat or WhatsApp, to social media networks like Facebook and Twitter, consumers now have a bevy of options to communicate over networks separate from traditional telephone and cellular calls. These advances have made it easier and cheaper for people to connect with each other around the world.

However, as breaches of consumer data continuously confront us, we must ensure the rules and regulations protecting consumer information are up to date and applied equally across the Internet ecosystem. The FCC has tried to keep up with the technological innovations over the past 20 years, but an outdated statute limits their efforts. It is crucial we protect consumer's sensitive information, no matter the means of communications, and without hampering innovation.

I look forward to discussing how we can effectively update the law to conform to the challenges and opportunities of the digital age.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Doyle, you are recognized for 5 minutes.

OPENING STATEMENT OF HON. MICHAEL F. DOYLE, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

Mr. DOYLE. Thank you, Madam Chair, for holding this hearing, and thank you to the witnesses for appearing before us today.

Digital privacy in our modern era has never been more important. And as our society becomes increasingly connected, it will become even more important. I believe that we can and must do more to protect American's privacy and sensitive information.

This committee's hearing with Facebook's CEO Mark Zuckerberg showed how concerned our members are with the practices of one of the world's largest tech companies. And what that hearing made clear was that the FTC does not have the manpower or authority to adequately enforce its own consent decree against Facebook, let alone proactively police this fast-evolving space.

To solve this problem and to give the American people the protections they are demanding, we are going to need a comprehensive solution that includes more resources, more manpower, and more authority to go after bad actors, and the ability to set rules of the road for the digital economy.

Facebook demonstrated all too well that after-the-fact-enforcement authority can't help us when the damage has already been done.

Europe's implementation of its GDPR rules, as well as California's recently and quite quickly passed privacy law, are clear indications that people at home and abroad recognize the need for strong privacy protections. We in Congress and on this committee need to take that to heart as we are addressing this pressing issue.

Now, with regards to today's hearing and the topic before us, CPNI, or Customer Network Proprietary Information, the FCC en-

forces the CPNI rules under section 222 of the Communications Act. This section restricts how telecommunications carriers can use and share customer data related to their service. This section and the authority it grants the Commission are some of the strongest privacy laws we have in this country and are intended to give consumers a modicum of protection.

These rules were expanded in 2016 to include broadband services as well. Those rules too were simple but effective.

The three components were, first, if your broadband provider wanted to use your data, it had to ask your permission. Secondly, it had to take reasonable steps to protect that data. And third, it needed to notify you if your data was breached.

These rules were an expansion of the FCC's existing CPNI rules and would have meaningfully enhanced our nation's privacy laws. However, Chairman Blackburn cosponsored and successfully led an effort to repeal these simple, sensible rules. As of yet, there has been no replacement.

The majority cannot claim that it values privacy when one of its signature achievements this Congress is the repeal of these meaningful rules.

Americans around the country are shouting for more, not less, privacy protections. Whether it is through ballot initiatives, billboards, people want more control over their digital lives. This is why it is so concerning that the FCC is doing so little to enforce its existing protections under section 222.

Thanks to the work by Senator Wyden and his staff, we recently discovered that real-time location of hundreds of millions of cell phones were being made available by our nation's wireless carriers without consumers' consent.

At least one company, Securus, used their access to this data to create a service for tracking and locating nearly every cell phone in real time. On top of that, Securus forced families calling prisons to consent to have their location tracked as a condition for talking on the phone with their incarcerated family members. This seems like no choice at all.

LocationSmart, the data aggregator that made this data available, had such poor security on their website that according to a researcher at Carnegie Mellon University, individuals could look up real-time location data with little effort.

These carriers it seems trusted but did not verify that consumers were giving consent to be tracked, and that gross negligence on their part exposed supposedly protected sensitive data to hundreds of millions of people.

These revelations are deeply troubling, but what is more troubling is the lack of knowledge by the FCC of what appears to be a pervasive practice in the wireless industry.

Similar to the Facebook incident, we still don't even know the extent of this breach and who may have had access to this data.

Madam Chairman, I would respectfully request that this committee hold a hearing on this incident to understand how it happened and to hold the responsible parties accountable.

With that, I will yield back the remainder of my time, and I look forward to the testimony of our witnesses.

[The prepared statement of Mr. Doyle follows:]

PREPARED STATEMENT OF HON. MICHAEL F. DOYLE

Thank you, Chairman Blackburn, for holding this hearing—and thank you to the witnesses for appearing before us today.

Digital privacy in our modern era has never been more important, and as our society becomes increasingly connected it will become even more important. I believe that we can and must do more to protect American's privacy and sensitive information. This Committee's hearing with Facebook's CEO Mark Zuckerberg showed how concerned our members are with the practices of one of the world's largest tech companies.

What that hearing made clear was that the FTC does not have the manpower or authority to adequately enforce its own consent decree against Facebook, let alone pro-actively police this fast-evolving space. To solve this problem and to give the American people the protections they are demanding, we are going to need a comprehensive solution that includes more resources, more manpower, more authority to go after bad actors, and the ability to set rules of the road for the digital economy. Facebook demonstrated all too well that after-the-fact enforcement authority can't help us when the damage has already been done.

Europe's implementation of its GDPR rules, as well as California's recently and quite quickly passed privacy law, are clear indications that people at home and abroad recognize the need for strong privacy protections. We in Congress and on this Committee need to take that to heart as we address this pressing issue.

Now, with regard to today's hearing and the topic before us, CPNI or Customer Network Proprietary Information: The FCC enforces CPNI rules under Section 222 of the Communications Act. This section restricts how telecommunications carriers can use and share customer data related to their service. This section and the authority it grants the Commission are some of the strongest privacy laws we have in this country and are intended to give consumers a modicum of protection.

These rules were expanded in 2016 to include broadband services as well. Those rules too were simple, but effective. The three components were: first if your broadband provider wanted to use your data, it had to ask your permission, second it had to take reasonable steps to protect that data, and third it needed to notify you if your data was breached. These rules were an expansion of the FCC's existing CPNI rules and would have meaningfully enhanced our nation's privacy laws. Chairman Blackburn cosponsored and successfully led the effort to repeal these simple, sensible rules; as of yet there has been no replacement. The majority cannot claim that it values privacy when one of its signature achievements this Congress is the repeal of these meaningful rules.

Americans around the country are shouting for more not less privacy protections; whether it is through ballot initiatives or billboards, people want more control over their digital lives. That is why it's so concerning that the FCC is doing so little to enforce existing protections under Section 222. Thanks to work done by Senator Wyden and his staff, we recently discovered that the real-time location of hundreds of millions of cell phones were being made available by our nation's wireless carriers without consumer's consent.

At least one company, Securus, used their access to this data to create a service for tracking and locating nearly every cell phone in real time. On top of that Securus forced families calling prisons to consent to have their location tracked as a condition for talking on the phone with their incarcerated family member. That seems like no choice at all.

Location Smart, the data aggregator that made this data available, had such poor security on their website that, according to a researcher at CMU, individuals could lookup real-time location data with little effort. The carriers, it seems, trusted but did not verify that consumers were giving consent to be tracked, and that gross negligence on their part exposed the supposedly protected sensitive data of hundreds of millions of people.

These revelations are deeply troubling, but what's more troubling is the lack of knowledge by the FCC of what appeared to be a pervasive practice in the wireless industry. Similar to the Facebook incident, we still don't even know the extent of this breach and who may have had access to this data.

Madam Chairman, I would respectfully request that this Committee hold a hearing on this incident to understand how it happened and to hold the responsible parties accountable. With that I yield back the remainder of my time and look forward to the testimony of our witnesses.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Walden has not arrived. Does any member on the Republican side seek to claim his time?

Seeing no one, I will go to—Mr. Pallone is not here.

Does anyone on the Democrat side seek to claim his time?

Ms. Eshoo, you are recognized.

OPENING STATEMENT OF HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. ESHOO. Thank you, Madam Chairwoman. And thank you to the witnesses. It is good to see each one of you.

I was surprised when the majority actually called this hearing. I think that there is an urgent need to examine privacy and data protections across the internet ecosystem, but I think this hearing, most frankly, is being held under disingenuous pretenses, and that the majority is inaccurately portraying itself as champions of consumer privacy reform when the record shows otherwise. Mr. Doyle raised this in his opening statement.

In fact, the only action the majority has taken on privacy to date has been to actively roll back existing privacy protections and expose consumers to increased harm. Consumers legitimately feel that they have completely lost control of their personal information. There is not a single one-size-fits-all solution to this, but in 2016, I think we were making progress. That is when the FCC extended CPNI protections to apply to broadband access services. That was a step forward for consumers. It should have been the first step toward protecting privacy at other points in the digital economy, including at the Edge.

But instead, the majority pushed through a partisan repeal of the rules before the ink was even dry on a razor-thin vote of 215 to 205 with 15 Republicans opposed. Everyone on this committee remembers what a bitter fight that was. But in the end, there were pressures that beat out consumer protection. So now as a result, there are currently no strong privacy rules anywhere in the digital ecosystem.

Americans have spent the last 17 months completely vulnerable to privacy exploitation and data breaches without recourse. Our most sensitive information, location data, medical history, Social Security numbers and mothers' maiden names are daily transmitted through networks of companies who no longer have any meaningful obligation to protect it. And I think that the American people are legitimately outraged by this.

So, Madam Chairwoman, I fully support real attempts. And I underscore that word, "real attempts" to seek meaningful solutions for privacy protection across the diverse internet economy. And I think our witnesses here today are going to help to inform our thinking.

So with that, I yield back the balance of my time, and I want—yes. Oh, Jerry. I will be happy to yield to my colleague from California, Mr. McNerney.

Mr. MCNERNEY. Well, I thank my colleague for yielding.

Despite demands from Americans for more control over the information they share online, last year, Republicans in Congress voted to strip consumers of the power to choose how ISPs use and share

their information. Republicans also voted to eliminate important data security protection for consumers.

Now, ISPs are no longer required to take even reasonable steps to secure consumers' personal information. Given the growing cyber threats that our Nation faces, it is critical that we do more and not less to secure consumers' data. That is why I introduced the MY DATA Act, which would give the Federal Trade Commission important tools to protect consumers' privacy and security online. I hope that we can work together to move the MY DATA Act forward.

And does the ranking member wish some time?

Mr. PALLONE. Well, let me just say, if I could. Madam Chair, if I could ask unanimous consent to include my statement in the record.

Mrs. BLACKBURN. Without objection.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Privacy is a deeply held American value. Today, location data is collected not only by phone companies, but by apps and phone operating systems. According to a recent Harris poll, 78 percent of people believe that a company's ability to protect their privacy is "extremely important," but only 20 percent "completely trust" companies to maintain the privacy of their data. This is not surprising considering all of the recent privacy breaches, including the Cambridge Analytica scandal. That is why I called for hearings so we can directly question executives from tech companies, internet service providers, data brokers and other companies that collect our information.

Unfortunately, as Americans were demanding greater privacy protections, Republicans eliminated existing privacy rules and they continue to show little appetite for meaningful reform. Two years ago, the FCC adopted strong privacy rules for internet service providers under Section 222 of the Communications Act. Instead of embracing those rules, one of the first acts of the Republican Congress and the Trump Administration was to repeal them. Consumers need strong privacy protection across the entire Internet ecosphere, which is broader than just ISPs, but eliminating ISP privacy protections just left Americans less safe and angry.

It was only after a huge public uproar and protests back in their districts that Republicans put forward a weak and unacceptable alternative. Ms. Blackburn's bill lacks basic protections such as rulemaking authority and significant civil penalties. And even this watered-down proposal has garnered little support from Republicans. It's no wonder that states like California are stepping in to fill the void left by the repeal of these privacy rules. And now that Republicans have rolled back not only online privacy protections, but also net neutrality, the FCC is left with limited authority to protect privacy. For telecommunications companies, the CPNI rules do remain. These rules require providers to protect information like a caller's name, location, who they called, and for how long. These are strong rules, but they are only effective if the FCC aggressively enforces them, which Chairman Pai has not.

According to recent news reports, third-party data aggregators, such as LocationSmart and Securus, obtained real-time location data from wireless carriers and allowed access to that data in ways that appear to violate the CPNI rules. This appeared to be happening for a long time. Fortunately, the FCC opened an investigation into LocationSmart, but why did it take so long? Why did it take a Canadian security researcher to identify the problem? And what is the FCC doing to proactively identify potential violations of its CPNI rules? These questions deserve answers, and that's why I've called for a hearing on this incident.

In another move that puts companies before consumers, tomorrow, the FCC is considering eliminating the agency's traditional role in helping consumers resolve informal complaints.

Currently, the informal complaint process is a free and easy way for consumers to use the FCC's help resolving everyday problems with communications companies.

Chairman Pai is proposing that the FCC now just simply pass the consumer's complaint to the company. And then if the customer is unsatisfied, they will be encouraged to file a $225 formal complaint.

This is simply not right. The FCC should work for consumers, not make life harder for them. That's why Ranking Member Doyle and I sent a letter to the Commis-

sioners yesterday urging them not to limit the ability of FCC staff to help resolve consumers' complaints. At a time when every dollar matters to working class families, it should be among the Commission's highest priorities to help consumers on the losing end of a growing imbalance of power.

With that, I yield the balance of my time.

Mr. PALLONE. Thank you.

Mr. MCNERNEY. I yield back.

Mrs. BLACKBURN. The gentleman yields back. The gentlelady yields back. And that concludes member opening statements.

And I would like to remind all members that pursuant to the committee rules, all members' opening statements will be made a part of the record.

We want to thank our witnesses for being here today and taking time to be before the subcommittee. Today's witnesses will have the opportunity to give their opening statements, followed by a round of questions from members.

On our panel today we have Mr. Hance Haney, director and senior fellow at the Technology and Democracy Project at the Discovery Institute. Mr. Rob McDowell, senior fellow at the Hudson Institute, and a former FCC commissioner. And I think she may get the prize for most appearances this year; Ms. Laura Moy, deputy director of the Georgetown Law Center on Privacy and Technology.

We appreciate each of you being here, making your testimony available to us.

We will begin today with you, Mr. Haney. You are now recognized for 5 minutes for an opening statement.

STATEMENT OF HANCE HANEY, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND DEMOCRACY PROJECT, DISCOVERY INSTITUTE; ROBERT MCDOWELL, SENIOR FELLOW, HUDSON INSTITUTE, FORMER COMMISSIONER, FEDERAL COMMUNICATIONS COMMISSION; AND LAURA MOY, DEPUTY DIRECTOR, GEORGETOWN LAW CENTER ON PRIVACY AND TECHNOLOGY

STATEMENT OF HANCE HANEY

Mr. HANEY. Thank you very much, Chairman Blackburn, Ranking Member Doyle, and Ranking Member Pallone.

Section 222 of the Communications Act requires telecommunications common carriers to obtain customer approval in order to use, disclose, or permit access to Customer Proprietary Network Information.

CPNI consists of call detail information, including the time, location, duration of telephone calls, as well as the telephone numbers from which calls originate and terminate. It also includes billing and other information.

Section 222 does not apply to broadband services, which are classified as an information service. Even though broadband services could be thought of as being provided by telecommunications carriers, the statute and the regulations look to the service provided, not to the provider of the service.

Instead, broadband is subject to the unfair and deceptive acts and practices authority of the Federal Trade Commission. This is the same authority that governs video streaming services, search

engines, social networking sites, e-commerce sites, and user-generated media sites.

The FTC privacy framework is technology neutral and it identifies categories of sensitive information that may give rise to an obligation by companies to obtain affirmative, express customer consent, otherwise referred to as opt-in approval.

Sensitive information includes information about children, financial and health information, Social Security numbers, and precise geolocation data, according to the FTC.

Technology neutrality is appropriate because, as the FTC has observed, broadband providers are no different than other participants in the internet ecosystem in terms of their ability to collect and utilize information about consumers.

The FTC's recognition that the requirement to use opt-in should be limited is also appropriate. Due to consumer inertia, most consumers typically don't take action in this type of situation. The requirement to obtain opt-in approval can be costly and inefficient, even a barrier to innovation.

Consumers benefit from the use of information that companies see and collect in the course of serving their customers, as companies like Google have demonstrated. Advertising underwrites the cost of services that Google offers for free to the public, and there is no reason that advertising couldn't also help offset the cost that broadband providers incur in offering broadband service.

Privacy regulation involves transaction costs and may have anticompetitive consequences if it is applied unevenly. Ideally, all market participants should be subject to a uniform privacy framework administered by a single agency for the sake of consistency.

The FTC's current privacy enforcement practice satisfies these criteria. Admittedly, making the internet more secure will likely always be a work in progress, and there is a role for both market solutions as well as regulation.

Legislation to enhance consumer privacy protection, if any, should strive for technological and competitive neutrality. In particular, it isn't rational to subject some market participants to heightened privacy regulation just because they were subject to economic regulations in the past.

We live in an era of rapid technological convergence in which it is wise to consider that every participant in the internet ecosystem is a potential competitor at least to some extent. Moreover, privacy protection should be calibrated according to the sensitivity of the information at issue in recognition of the fact that there are transaction costs associated with consumer consent systems.

Opt-in systems are particularly burdensome and should be reserved for only the most sensitive personal information. Where customer information is less sensitive, consumers' privacy expectations should be balanced with the benefits consumers are likely to derive from a dynamic, competitive market, including greater abundance of choices and lower prices. Such a market is one where all providers have similar opportunities to innovate and earn a fair return on investment.

Finally, to the extent possible, regulation should reflect the practical reality that it is difficult to make predictions about how the market will evolve and at what pace, and that the process of cali-

brating regulation on an ongoing basis as necessary to reflect changes in the market can be slow.

Thank you.

[The prepared statement of Mr. Haney follows:]

Testimony of

Hance Haney
Director and Senior Fellow
Technology & Democracy Project
Discovery Institute

Before the

Subcommittee on Communications and Technology
Committee on Energy and Commerce
House of Representatives

On

Protecting Customer Proprietary Network Information in the Internet Age

July 11, 2018

Dear Chairman Blackburn, Ranking Member Doyle and Members of the Subcommittee,

Section 222 of the Communications Act of 1934, as amended, governs the privacy practices of telecommunications common carriers, including local, long distance, commercial mobile wireless service (CMRS) and interconnected voice-over-Internet Protocol (VoIP) providers, such as AT&T, Sprint, and Verizon. Among other things, carriers are generally prohibited from using, disclosing or permitting access to individually identifiable customer proprietary network information (CPNI) without customer approval.[1]

CPNI is defined as: 1) information relating to the "quantity, technical configuration, type destination, and amount of use" of a telecommunications service received by a particular customer and 2) information pertaining to telephone exchange and telephone toll service contained in the

[1] 47 U.S.C. §222(c)(1).

billing that a customer receives.[2] CPNI includes, with some exceptions, "virtually all information about a customer's use of network services" that a telecommunications carrier may acquire from providing those services.[3] Examples of CPNI include detailed descriptions of voice calling history (including the time, location and duration of the call, as well as the telephone numbers from and to which the call was placed),[4] and the products and services purchased or subscribed to by an individual customer—such as call waiting, caller I.D. and call forwarding.[5] There are exceptions to the rule.

Among the exceptions, telecommunications carriers are permitted to use, disclose or permit access to CPNI *without* customer approval in the course of marketing service offerings to their current customers, provided those services are within the carrier's own "category" of service.[6] The service categories are: local, long distance and wireless. Thus, telecommunications carriers may not use any CPNI in their possession to market to a prior customer who switched to another carrier, or market to customers who are receiving another category of service from another provider. Otherwise, in order to use, disclose or permit access to CPNI for the purpose of competing in the marketplace, carriers have to obtain "opt-in" approval (*i.e.,* the carrier must obtain affirmative, express consent in advance from the customer). Carriers may obtain approval through written, oral or electronic methods, but they bear the burden of demonstrating that oral approval has been given in compliance with FCC rules, and they must maintain records of approval—whether oral, written or electronic—for at least one year.[7]

---

[2] *Id.,* at §222(h)(1).
[3] Peter W. Huber, *et al.* Federal Telecommunications Law (2d. Ed.) (Aspen Law & Business, 1999) at 438.
[4] 47 C.F.R. §64.2003(d).
[5] *Id.,* at §64.2005(c)(3).
[6] *Id.,* at §64.2005(a).
[7] *Id.,* at §64.2007(a).

Broadband

Section 222 does not apply to broadband services, which are classified as an "information" service.[8] Therefore, even though broadband services could be thought of as being provided by telecommunications carriers, the statute and the regulations look to the service provided, not to the provider of the service. Accordingly, broadband is excluded from the ambit of Title II of the Act—including Section 222 and the FCC's CPNI rules. Instead, broadband is subject to the unfair and deceptive acts and practices authority of the Federal Trade Commission (FTC). This is the same authority that governs video streaming services like Netflix and YouTube, search engines like Google and Bing, social networking sites like Facebook and LinkedIn, e-commerce sites like Amazon and eBay and user-generated media sites like Twitter and Pinterest (*i.e.,* the entire Internet ecosystem). In other words, none of the services I have referenced here fit within the statutory definition of CPNI.

The FCC concluded in 2015 when it briefly classified broadband as a "telecommunications" service that the CPNI rules, which were designed to address concerns relating to voice service, were not well suited to broadband Internet access service.[9] The CPNI rules—as they were then and are now—do not address "many of the types of sensitive information to which a provider of broadband Internet access service is likely to have access," according to the Commission, "such as (to cite just one example) customers' web browsing history."[10] A leading industry participant expressed the opinion that it was "unclear what these privacy protections would even mean in the broadband context…"[11]

---

[8] *Restoring Internet Freedom,* WC Docket N. 17-108, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd 311 (2018) (*Internet Freedom Order*).
[9] *Protecting and Promoting the Open Internet*, WC Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5823-24 , para. 467 (2015) (*Title II Order*).
[10] *Id.*
[11] Verizon *Ex Parte* Letter at 7-8, GN Docket No. 14-28 (Jan. 26, 2015).

The *Privacy Order* adopted by the FCC in October 2016 modified the CPNI rules to account for the unique aspects of broadband service offerings, which were classified as a telecommunications service at the time.[12] The *Privacy Order* created a stricter privacy framework for broadband service providers than for other participants in the Internet ecosystem—creating asymmetric regulation that could inhibit competition and jeopardize private investment in broadband networks. Specifically, carriers were required to obtain opt-in consent in order to use, disclose or permit access to virtually all information about a broadband customer's use of the network for purposes such as marketing or advertising. In March 2017, Congress voted to disapprove the FCC's 2016 *Privacy Order* pursuant to the Congressional Review Act, which prevents the FCC from adopting another set of rules in substantially the same form.[13]

FTC Privacy Framework

Presently, all companies in the Internet ecosystem are subject to the Federal Trade Commission's privacy enforcement practice. The FTC privacy framework is technology neutral, and identifies categories of "sensitive" information that may give rise to an obligation by companies to obtain affirmative express customer consent (opt-in). Sensitive information includes: information about children, financial and health information, Social Security numbers, and precise geolocation data, according to the FCC.[14] Opt-in should be sought, for example, where a company's business model "is designed to target" consumers based on sensitive data, reasons the FTC, however risks to consumers may not justify the burdens that opt-in would entail for general audience businesses that "incidentally collect" sensitive information.[15]

---

[12] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* Report and Order, 31 FCC Rcd 13911 (2016) (*Privacy Order*).
[13] *See* Pub. L. No. 115-22 (Apr. 3, 2017); *see also* 5 U.S.C. § 801(b)(2).
[14] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* at 47 (Mar. 26, 2012), *available at* http://go.usa.gov/csYRz
[15] *Id.*

Technology neutrality is appropriate, because as the FTC has observed, broadband providers (also referred to as Internet Service Providers, or ISPs) are no different than other participants in the Internet ecosystem in terms of their ability to collect and utilize information about consumers.

> ISPs are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity. Like ISPs, operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles.[16]

The FTC's recognition that opt-in should be limited is also appropriate. Consumers benefit from the use of information that companies see and collect in the course of serving their customers, as companies like Google have demonstrated. Advertising underwrites the cost of services that Google offers for free to the public, and there's no reason that advertising couldn't help offset the cost that broadband providers incur in offering broadband service (broadband providers should therefore be viewed as potential competitors to companies such as Google).[17] The *Privacy Order* would have foreclosed this possibility by requiring broadband providers to obtain opt-in approval to use customer data in the same manner as Google, although Google itself is under no similar obligation.

Opt-in typically results in substantially lower rates of consent than an opt-out system, because most of the time consumers take no action.[18] For example, in attempting to comply with the CPNI opt-in requirement, the former Regional Bell Operating Company U S WEST—at one time the primary provider of local exchange telephone service in 14 western states—obtained an

---

[16] *Id.*, at 56.
[17] "Google CEO sees free cell phone service," *Reuters* (Nov. 13, 2006) ("'Your mobile phone should be free,' Schmidt told Reuters. 'It just makes sense that subsidies should increase' as advertising rises on mobile phones."), *available at* https://www.reuters.com/article/businesspro-google-ceo-dc/google-ceo-sees-free-mobile-phones-funded-by-ads-idUSL0972867220061112.
[18] Huber, Fed. Telecom. Law, *supra* note 3.

opt-in rate of only 29 percent among it's residential subscribers at a cost of $20.66 per positive response.[19] Obtaining opt-in approval can be costly and inefficient compared to the alternatives (*e.g.,* inferred consent or opt-out consent, which do not require consumers to take action). Accordingly, it is anticompetitive if the most burdensome consent system is not applied equally to all market participants. Consumers are harmed when competition is lessened.

Different sets of rules for different firms (*i.e.,* asymmetrical regulation) can have anticompetitive consequences—or what the FCC chose to call "ripple effects" in the *Privacy Order* proceeding.[20] The goal should be to prevent regulations from hamstringing some market participants but not others, and the logical way to do that is by ensuring that all participants in the Internet ecosystem are treated the same. The FTC privacy framework, which applies to all participants in the Internet ecosystem, achieves this objective.

The *Privacy Order* justified asymmetric regulation on the ground that edge providers only get to see a "slice" of any given consumers Internet traffic, while broadband providers get to see 100 percent of a customer's *unencrypted* Internet traffic.[21] Encryption makes the Internet safer from eavesdropping, content hijacking, cookie stealing and censorship, according to the Electronic Frontier Foundation.[22] Encryption protected 77 percent of requests sent from computers around the world to Google's servers, for example, as of February 27, 2016.[23] By June 23 of this year,

---

[19] Thomas Lenard and Scott Wallsten, An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking, *Technology Policy Institute* at 27 (May 2016), *available at* https://techpolicyinstitute.org/wp-content/uploads/2016/05/Lenard_Wallsten_FCCprivacycomments.pdf (the authors observe that transactions costs like the ones incurred by U S WEST in this instance are "ultimately paid by consumers, either through higher prices or reduced services and benefits").

[20] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd 2500, 2546, para. 132 (2016) (*Broadband Privacy NPRM*).

[21] *Privacy Order, supra* note 12, 13920, para. 30.

[22] "We're Halfway to Encrypting the Entire Web," by Gennie Gebhart, Electronic Frontier Foundation (Feb. 21, 2017) *available at* https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web.

[23] "77 Percent of Google Internet Traffic Now Encrypted, by Angela Moscaritolo, *PC News* (Mar. 16, 2016) *available at* https://www.pcmag.com/news/342935/77-percent-of-google-internet-traffic-now-encrypted.

encryption protected 95 percent of Google's traffic.[24] Although not yet 100 percent pervasive across the entire Internet, particularly among smaller platforms, that's the direction encryption is heading. So in reality, the amount of a customer's encrypted Internet traffic that a broadband provider does not get to see is substantial, and the amount of unencrypted traffic it does get to see is shrinking. This is a perfect example of a market based solution that is eroding any justification for asymmetrical privacy regulation. The *Privacy Order* discounted encryption because it isn't 100 percent pervasive and ignored the fact that the use of encryption is clearly trending in that direction. Arguably, this is an example of government making unwarranted assumptions about how a dynamic market will evolve in order to pick winners and losers.

All participants in the Internet ecosystem gather valuable information in the course of serving their customers, and regulators will have to accept that the information that any particular participant, or class of participants, can gather may not be complete or identical to that which is available to other participants, and that in a perfect world companies would like to have direct access to all kinds of information that they do not. Markets are rarely perfectly competitive.

Rather than focus on the quantity and quality of customer information available to various market participants, the FCC in it's *Privacy* Order proceeding should have focused on whether there is, in fact, any harm to consumers from targeted advertising, and on how and why the existing FTC privacy framework may be unsuitable for broadband. The FCC had an obligation to set out why, from a consumer perspective, it's a materially more significant privacy threat for broadband service providers to know what websites a customer has visited, at what hours of day, from what location using which type of device than it is for a search engine to view search terms and click-throughs, and it failed to do so.

---

[24] "HTTPS encryption on the web," Google Transparency Report, *available at* https://transparencyreport.google.com/https/overview.

The Anticompetitive Purpose of Section 222.

When the FCC adopted CPNI rules in 1987, it specifically declined to adopt a "prior authorization" requirement like opt-in.[25] Sec. 222, enacted in 1996 in part to protect consumer expectations of privacy while facilitating information sharing between new entrants and incumbent providers who in most cases would be using many of the same facilities to serve their respective customers, but just as importantly—if not more so—it was "an important bulwark of the interconnection rules," designed to protect competing carriers from an "unscrupulous interconnector, also a competitor."[26] In particular, CPNI was intended to prevent the Regional Bell Operating Companies—who were the incumbent providers of local exchange service in most of the country, and who had traditionally not been permitted to offer long-haul interexchange toll (*i.e.*, long distance) services—from using billing data to "target the more lucrative long distance customers." The RBOCs were in possession of the data because they had provided billing services for the long distance carriers. The information became competitively useful to the RBOCs when they were finally allowed to offer their own long distance services. Long distance carriers felt it was anticompetitive for the RBOCs to be able to use customer information that would otherwise have been proprietary data belonging to the long distance carriers if the market had been competitive from the beginning. This is a competitor-focused perspective. Real consumer-focused privacy rules arguably would have allowed the RBOCs to immediately contact all of the lucrative long distance customers and offer them a better deal.

Requiring broadband providers to receive "opt-in" approval before they can use customer information for purposes such as targeted advertising, as the *Privacy Order* did, has only one

[25] Huber, Fed. Telecom. Law, *supra* note 3.
[26] Peter W. Huber, *et al.* The Telecommunications Act of 1996: Special Report (Aspen Law & Business, 1996), 54-55.

purpose and that is to make it harder for broadband providers to offer targeted advertising in competition with edge providers who would not have had to play by the same set of rules. Real consumer-focused privacy rules would not be aimed at protecting the competitors of the broadband service providers, but at ensuring that consumers can receive targeted ads from as many sources as possible. The Commission practices crony capitalism when it adopts rules that have the effect of picking winners and losers in the marketplace.

Investment Effect

The FCC argued during the *Privacy Order* proceeding that privacy regulation will *promote* broadband investment and deployment, because: a) the "largest investment ever in wireline networks came during those years in which DSL Internet access services were regulated under Title II," and b) "protection of privacy encourages broadband usage that, in turn, encourages investment in broadband networks."[27]

The second point is not the justification for new regulation that it may seem. If privacy protection encourages broadband usage and therefore promotes broadband investment, then broadband providers already have a natural incentive to protect privacy and FCC regulations are unnecessary.

The assertion that the largest investment in wireline networks occurred when DSL (*i.e.*, Digital Subscriber Line, or "dial-up," the technology that preceded broadband) was regulated under Title II is based on a flawed analysis by Free Press which looks at aggregate investment by incumbent and competitive local exchange carriers as well as wireless providers. Although all of these entities were covered under Title II, only the facilities of the incumbent local exchange carriers were subject to oppressive unbundling mandates that reduced incentives for investment in

[27] *Broadband Privacy NPRM, supra* note 20, 2505-06, para. 11.

last-mile facilities. Jeffrey A. Eisenach has observed that much of the pre-2000 investment was for marketing and operations, and that the elimination of unbundling in 2003-05 preceded an investment spike in broadband facilities.

> Since the FCC began exempting broadband infrastructures from unbundling requirements, overall investment in communications equipment in the U.S. has risen by more than 40 percent, as shown in Figure 2. And, unlike the prior investment bubble, much of which consisted of literally hundreds of billions "invested" by now bankrupt CLECs in advertising and overhead (Darby *et al* 2002), the bulk of the investment in the last five years has gone into network upgrades that have yielded a faster, more robust broadband infrastructure.[28]

The disastrous unbundling experiment that the Commission cited here—in which the Commission mandated artificially low prices for unbundled network elements that made it cheaper for new entrants to lease facilities from the incumbents rather than build their own, and which therefore required the incumbents to share any profits from successful investments and eat the entire loss from unsuccessful investments—illustrates why, for example, in the *Title II Order,* the Commission conceded that regulation can harm investment, and that "...deregulation often promotes investment..."[29] Moody's Investors Service also warned that broadband providers would be "severely handicapped" in their "ability to compete with digital advertisers such as Facebook and Google." The FCC disregarded this input when it adopted the *Privacy Order,* which buttressed the FCC's contrary conclusion on nothing more than an assessment by the National Consumers League that the industry had a strong financial year in 2015.[30]

Conclusion

Privacy regulation involves transaction costs and may have anticompetitive consequences if it is applied unevenly. Ideally, all market participants should be subject to a uniform privacy

---

[28] Eisenach, Jeffrey A., Broadband Policy: Does the U.S. Have it Right after All? (September 9, 2008). *available at* SSRN: http://ssrn.com/abstract=1265579.
[29] *Title II Order,* 5793-94, para. 414.
[30] *Privacy Order, supra* note 12, 13924, fn. 61.

framework administered by a single agency for the sake of consistency. The FTC's current privacy enforcement practice satisfies these criteria. Admittedly, making the Internet more secure will likely always be a work in progress, and there is a role for both market solutions as well as regulation.

Legislation to enhance consumer privacy protection, if any, should strive for technological and competitive neutrality. In particular, it isn't rational to subject some market participants to heightened *privacy* regulation just because they were subject to *economic* regulation in the past. We live in an era of rapid technological convergence, in which it is wise to consider that every participant in the Internet ecosystem is a potential competitor, at least to some extent. Moreover, privacy protection should be calibrated according to the sensitivity of the information at issue in recognition of the fact that there are transaction costs associated with consumer consent systems—opt-in systems are particularly burdensome and should be reserved for the only most sensitive personal information. Where customer information is less sensitive, consumer privacy expectations should be balanced with the benefits consumers are likely to derive from a dynamic, competitive market—where all providers have similar opportunities to innovate and earn a fair return on investment—including a greater abundance of choices and lower prices. Finally, to the extent possible, regulation should reflect the practical reality that it is difficult to make predictions about how the market will evolve and at what pace, and that the process of calibrating regulation on an ongoing basis as necessary to reflect changes in the market can be slow.

Mrs. BLACKBURN. The gentleman yields back.

Mr. McDowell, you are recognized.

STATEMENT OF ROBERT MCDOWELL

Mr. MCDOWELL. Thank you, Chairman Blackburn, Ranking Member Doyle, and Ranking Member Pallone as well, and distinguished members of the committee. It is an honor to be back before you here today.

I did serve as a Commissioner of the FCC from 2006 to 2013. Today, I am a partner at Cooley LLP, as well as co-leader of its communications practice, which is global. I am also a senior fellow at the Hudson Institute, as the chairman pointed out, and I testify today in my own capacity, and the views I express today are purely my own.

Sitting behind me is a remarkable young woman, as my aide-de-camp for the day. She is my daughter Mary-Shea Virginia McDowell. It is always good to have someone watching your back when you are in Washington, so——

Safeguarding sensitive or private information is a concept as old as human beings. The English term "eavesdropping" was created centuries ago when the ancestors of today's data thieves literally lingered under the eaves of roofs to listen to the private conversations of others.

Fast forward to 1980 when the FCC extended itself into the privacy arena in a narrow way as part of its computer inquiry proceedings. It issued rules governing what is now dubbed Customer Proprietary Network Information, or CPNI—could use some branding work on that name, I think—mainly as a safeguard against regulated monopoly local phone companies from using sensitive customer data to help their unregulated affiliates compete against new entrants at the time.

Then Congress codified section 222 in 1996, mandating the Commission to adopt more specific CPNI protection rules applicable only to common carriers. Since then, dramatic changes have occurred in the telecommunications, media, and technology, or TMT marketplace.

The maturation of the internet ecosphere, especially the mobile internet, has produced consumer benefits that were unimaginable 22 years ago when section 222 was codified. And America has led the way in these innovations.

Furthermore, the mobile net has also helped spark trillions of dollars in American economic growth. Brilliant engineers and intrepid entrepreneurs have invented new tools that have dramatically altered and improved our daily lives, forcing business models to experiment and converge.

Section 222, however, has remained the same despite these new market realities. Only telecommunications carriers must live under this law governed by the FCC, while the rest of the players in the dynamic internet ecosphere operate under privacy standards administered by the Federal Trade Commission.

This duality has created a legal and regulatory asymmetry in the diverse internet market. Additionally, America's public policy has evolved to create a regulatory regime that sometimes does not focus as much on the sensitivity of the data that is collected, but rather,

it focuses on what kind of market player collects the data. This approach could be more confusing for consumers, including myself, and companies alike, than would having one set of technology neutral rules that apply consistently across all platforms, including those we can't even imagine today.

Only Congress has the authority to modernize privacy and consumer protection laws to reflect the realities of the 21st century internet marketplace. I respectfully suggest that Congress examine a modernized and harmonized privacy framework that is technology neutral and which focuses on the sensitivity of the data that is collected, rather than the type of entity that collects the data.

That said, any uniform standard should guard against imposing overreaching or unnecessary regulations to help maintain America's leadership in the global TMT economy.

Thank you again for inviting me to appear before you today, and I look forward to your questions.

[The prepared statement of Mr. McDowell follows:]

STATEMENT
OF
THE HON. ROBERT M. MCDOWELL
SENIOR FELLOW
HUDSON INSTITUTE

"PROTECTING CUSTOMER PROPRIETARY NETWORK INFORMATION IN THE INTERNET AGE"

BEFORE THE
U.S. HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY
UNITED STATES HOUSE OF REPRESENTATIVES

JULY 11, 2018

HUDSON INSTITUTE
1201 PENNSYLVANIA AVENUE, N.W.
SUITE 400
WASHINGTON, DC 20004

Executive Summary

The story of the evolution of the Federal Communications Commission's rules governing "customer proprietary network information," or "CPNI," dates back to 1980, before the break-up of the AT&T "Ma Bell" phone monopoly when analog voice calls traveled over circuit-switched copper wires. Marty Cooper's cellular telephone invention was in its commercial infancy, and the Internet was an obscure computer-to-computer communications tool enjoyed by only a few thousand academics and government officials.

The FCC has modified its CPNI rules many times over the ensuing decades, with Congress last providing direction 22 years ago with the Telecommunications Act of 1996, specifically Section 222.[1] The FCC subsequently adopted rules to implement Section 222 on several occasions. When I served as commissioner, in 2007 I worked on a bipartisan basis with my colleagues on a partial restructuring of our CPNI rules.

Since then, dramatic changes have occurred in the telecommunications, media and technology ("TMT") marketplace. The maturation of the Internet ecosphere, especially the mobile Internet, has produced consumer benefits that were unimaginable 22 years ago. The mobile Net has also sparked trillions in American economic growth. While brilliant engineers and intrepid entrepreneurs invented new tools that have dramatically altered and improved our daily lives, business models have converged. Section 222, however, has remained the same despite these new market realities. Only telecommunications carriers must live under this law governed by the FCC while the rest of the players in the dynamic Internet ecosphere operate under privacy standards administered by the Federal Trade Commission. This has created a legal and regulatory asymmetry in the diverse Internet market.

Only Congress has the authority to modernize and harmonize privacy and consumer protection laws to reflect the realities of the rapidly-changing 21st Century Internet marketplace.

***

[1] Cable companies must protect customers' video viewing data under Section 631, a section that is similar in spirit to Section 222. 47 U.S.C. § 551.

CPNI and the 21st Century Digital Marketplace

Chairman Blackburn, Ranking Member Doyle, and distinguished Members of the Subcommittee, thank you for having me testify before you today. My name is Robert McDowell. I served as a commissioner of the Federal Communications Commission (FCC) from June 1, 2006, to May 17, 2013. I am a partner at Cooley LLP as well as co-leader of its global communications practice. I am also a Senior Fellow at the Hudson Institute. I testify today in my own capacity. The views expressed today are purely my own.

During my seven years at the FCC, we repeatedly examined issues related to "customer proprietary network information, or "CPNI,"[2] including adopting major reforms in 2007. As I said in 2007, the FCC's CPNI policies must "strike a careful balance," protecting consumers while "guard[ing] against imposing over-reaching and unnecessary" requirements on carriers.[3] The history of CPNI at the FCC reflects the struggle to maintain that balance in a changing communications environment. The Federal Trade Commission ("FTC") has been addressing the same issues for services under its jurisdiction, which include all services other than common carriage.

---

[2] Section 222 of the Communications Act of 1934 defines CPNI as:

> (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
>
> (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;
>
> except that such term does not include subscriber list information.

47 U.S.C. § 222(h)(1).

[3] Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115 and WC Docket No. 04-36, April 2, 2007. Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115, WC Docket No. 04-36, 22 FCC Rcd 6927 (2007).

Today, broadband Internet access services providers are once again subject to the same privacy regime as "edge" providers under the purview of the expert agency for privacy policy: the Federal Trade Commission. If a broadband provider has a corporate affiliation with a telecommunications carrier, then the carrier side of the business must also abide by the FCC's CPNI rules that protect sensitive information such as call records. Similarly, cable providers must protect video viewing information pursuant to Section 631.[4] Edge providers do not have these dual sets of regulations to govern their behavior or protect sensitive consumer data. Thus, as the telecommunications, media and technology ("TMT") marketplace converges, a legacy legal and regulatory asymmetry still exists that only Congress can reconcile. America's public policy has evolved to create a regulatory regime that does not focus as much on the *sensitivity* of the data that is collected, but, rather, it focuses more on what kind of market player collects the data. This approach can be more confusing for consumers and companies alike than would having one set of technology-neutral rules that apply consistently across all platforms.

The FCC first adopted rules concerning customer proprietary network information ("CPNI") in 1980 as part of its *Computer Inquiries.* Those proceedings created a framework to permit AT&T, the regional Bell operating companies, and GTE to provide what were then known as "enhanced services" (and now are called "information services") in competition with companies that did not provide telephone service. As the FCC explained in 1998, those rules were intended to "prohibit" the use of "CPNI obtained from . . . provision of regulated services to gain a competitive advantage in the unregulated CPE and enhanced services markets." Even then, the FCC also recognized that the rules would "protect legitimate customer expectations of confidentiality[.]"[5] The original rules

[4] 47 U.S.C. § 551.

[5] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; and Implementation of the Non-Accounting Safeguards of*

prohibited the *regulated* businesses of the Bell companies and AT&T from providing CPNI to their *unregulated* affiliates unless the information was available to the public. The FCC also adopted a parallel rule to prevent the Bell companies and GTE from sharing CPNI with their wireless affiliates.

Protection for CPNI was added to the Communications Act of 1934 in the Telecommunications Act of 1996 under a new Section 222. That section now sets the basic framework for handling customer-specific information generated by telecommunications providers. Under that framework, carriers are required to protect the confidentiality of CPNI. They can use CPNI to provide and bill for services, to prevent fraud, and to aid 911 operators and other public safety agencies. With customer permission, carriers can use CPNI to market other services. Carriers also can use aggregated CPNI that does not identify individual customers for marketing and can use customer names, addresses, and telephone numbers to create telephone directories, including Yellow Pages directories.

The FCC adopted rules to implement Section 222 in several orders from 1996 to 1998. Those rules divided services offered by carriers into several categories, with different levels of customer approval required for different services. Customer approval was not required to use CPNI to market services within the categories of telecommunications services the customer already was purchasing from the company, such as local exchange service or wireless service. Express customer approval was required for any other use of CPNI to market information services or other telecommunications services to that customer. The FCC also adopted rules to limit how carriers could use information they obtained when their customers were switching to other carriers.

Sections 271 and 272 of the Communications Act of 1934, as amended, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8070 (1998).

In 1999, the U.S. Court of Appeals for the Tenth Circuit overturned the requirement that telecommunications carriers obtain express consent for use of CPNI.[6] The FCC responded in 2002. The Commission decided to allow carriers to use notice and "opt-out" consent prior to using CPNI to market "communications-related services" – local telephone service, long distance service, wireless service, Internet access, and customer-premises equipment – but continued to require affirmative customer consent before a carrier could disclose CPNI to unrelated third parties or to carrier affiliates that provide non-communications services.

The FCC revisited CPNI issues again in 2007,[7] when I was serving as a Commissioner, to address a surge in fraudulent access to CPNI and to bring interconnected voice-over-IP services ("VoIP," or services that act like traditional telephone services, with dialable telephone numbers) under the umbrella of the rules. The new rules required carriers to authenticate their customers before providing access to CPNI, with different requirements for in-person, telephone, and online access; and adopted a new obligation to report unauthorized access to customer information to the FBI, Secret Service, and affected customers. The rules tightened the limits on when carriers could provide CPNI to contractors and joint venture partners and required notice to customers when changes in account information occur. The new rules also required carriers to report annually on their efforts to protect CPNI, on customer complaints about unauthorized access, and any actions taken against data brokers.

None of these rules applied to Internet access services, or to any other information service (such as voice mail or email), which traditionally had been subject to the FTC's privacy regime. This changed in February 2015, when the FCC adopted an order that declared, for the first time, that

---

[6] *U. S. West, Inc. v. FCC,* 182 F.3d 1224 (10th Cir. 1999), *cert. denied,* 530 U.S. 1213 (June 5, 2000).

[7] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115, WC Docket No. 04-36, 22 FCC Rcd 6927 (2007).

broadband Internet access services would be regulated under Title II of the Communications Act of 1934 as common carriage services. One consequence of that decision was to subject broadband Internet access services to a host of common carrier obligations, including the CPNI requirements in Section 222, and to remove broadband providers from the FTC's authority. The FTC retained jurisdiction over other information services, such as "edge providers" that offer video, apps, gaming and some forms of voice communications.

In 2016, the FCC proposed to apply the existing CPNI rules (with some adaptations) to broadband Internet access services.[8] Late in the year, however, it decided instead to adopt a wholesale revision of the CPNI rules that used the sensitivity of customer information to determine how that information would be treated. Under that approach, opt-in approval from the customer was required before a carrier or broadband provider could use or share the most sensitive information, such financial, health, and precise geo-location information.[9] Opt-out approval was required for "non-sensitive information," and no approval was required for a carrier or broadband provider to use or share information that had been exempted from approval requirements by Section 222. The order also modified the data breach notification requirements to treat larger breaches differently than smaller breaches; prohibited providers from requiring customers to agree to use of their data as a condition of obtaining service; and permitted agreements between service providers and enterprise customers that did not comply with the rules. Again, only broadband service providers had to comply with these standards, not any other part of the Internet ecosphere, such as "edge" providers.

---

[8] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (2016).

[9] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Report and Order, 31 FCC Rcd 13911 (2016).

Congress overturned the 2016 rules under the Congressional Review Act in April 2017, and the FCC released an order reinstating the prior rules and noting that broadband Internet access remained subject to Section 222 in June 2017. In December 2017, the FCC reversed its 2016 decision to treat broadband Internet access as a common carrier service. As a result, broadband Internet access service, like any information service, no longer is subject to the FCC's CPNI requirements, and the 2007 rules continue to apply to telecommunications service and interconnected voice over IP service. Broadband Internet access service is once again subject to the FTC's privacy rules, however, providing consumers with the formidable protections of that agency.

Conclusion

The FCC and Congress have addressed CPNI issues repeatedly since the first rules were adopted in 1980. The rules have evolved as the industry and customer expectations have changed, and periodic re-examination of the rules to maintain the balance between customer privacy and legitimate business interests is appropriate. In the current environment, the FCC has jurisdiction over privacy for traditional telecommunications services and interconnected voice-over-IP services, while the FTC has jurisdiction over privacy for broadband Internet access and all other information services. Legacy laws, however, have created a legal and regulatory asymmetry just as markets are witnessing dramatic convergence and experimentation. Only Congress has the authority to modernize privacy and consumer protection laws to reflect the realities of the 21st Century Internet marketplace. I respectfully suggest that Congress examine a modernized and harmonized privacy framework that is technology neutral and which focuses on the sensitivity of the data versus the type of entity holding the data.

Thank you again for inviting me to appear before you today, and I look forward to your questions.

Mrs. BLACKBURN. The gentleman yields back.

Ms. Moy, you are recognized.

STATEMENT OF LAURA MOY

Ms. MOY. Thank you very much.

Good morning, Chairman Blackburn, Ranking Member Doyle, Ranking Member Pallone, and distinguished members of the committee.

So the subject of today's hearing is Customer Proprietary Network Information, sometimes referred to as CPNI, which I agree with Mr. McDowell that that may need some branding work. That is the information collected by telecommunications providers—and right now, that means just phone providers—about subscribers' use of the information. So important information about our communications, like who we call and who calls us, how often we call them, how long we talk to them, and where we are calling from.

And I am really glad we are having a hearing on CPNI because the law that protects CPNI is one of the strongest Federal consumer privacy laws we have. It requires phone carriers to get their customers' permission before using CPNI for purposes other than to provide the phone service. In other words, you are paying for your phone service, and your carrier simply delivers the service without always trying to make an extra buck off your private life.

So your phone carrier can't use the fact that you have been calling banks and credit card companies to market your payday loans, or the fact that you have been calling an elderly relative and healthcare providers more frequently to market your home health services, nor can it sell that information to outsiders without getting your permission first.

The CPNI privacy law also enables an expert agency to issue regulations that can be modified and updated in accordance with changing technology and business practices. And this is really important.

The CPNI privacy law also gives the FCC robust enforcement authority in the form of fines. And using this authority just in the last few years, the FCC has fined four different carriers for violations of CPNI privacy protections.

The CPNI privacy law should serve as a model for future privacy laws this Congress may consider because of its substantive strength, the regulatory flexibility it offers through rulemaking, and its enforcement strength.

But instead, however, the benefits to consumer privacy presented by the CPNI privacy law has faced some major setbacks. As multiple people in this room have mentioned, last year, Congress, including a number of members of this subcommittee, voted against the application of these strong privacy rules to broadband providers, even though, like the phone, broadband is now an essential service, and like phone carriers, broadband providers enjoy privileged insight into their subscribers' private communication.

And this year, as the FCC eliminated net neutrality rules, it removed broadband providers altogether from the reach of the CPNI privacy law, which, as I said, is one of the strongest consumer privacy laws we have on the books.

So that brings us to today, and here, as we consider what our path forward should be. It is clear that we must do something. Ninety-one percent of adults in America feel that consumers have lost control of their personal information. And nearly 70 percent thinks the law should do a better job of protecting their information.

Consumers want more privacy protection, not less. This is why the recent elimination of existing privacy protections was so unpopular among the American public.

As Congress considers how to give Americans the privacy protections they deserve, it should keep a few things in mind:

First, prospective rulemaking authority is an incredibly important consumer protection tool. After-the-fact enforcement can be helpful, but an enforcement-only regime does not always create clarity, and because it comes only after a problem has occurred, it does not necessarily protect consumers from the problem in the first place.

Granting rulemaking authority to an expert agency also fosters much needed regulatory flexibility. We don't always know what the next privacy or data security threat will be, but unfortunately, we all know that there will be one. An agency with rulemaking authority can respond to shifting threats more quickly than Congress can.

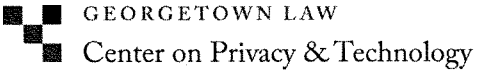
Second, consumer protections are only as good as their enforcement, so any new protections Congress creates on privacy or data security must be accompanied by strong enforcement authority.

Right now, the FTC does use substantial work on privacy and data security. But with few exceptions, it does not have the ability to seek civil penalties for privacy and data security violations. In fact, FTC staff and commissioners have appeared before Congress requesting civil penalty authority to buttress their authority. Agencies that are tasked with protecting consumers' private information cannot do it without the proper tools. Civil penalty authority is needed.

Third, Congress should avoid the temptation to address complex challenges with the one-size-fits-all approach. There are different types of actors on the internet with different roles to play, different relationships with and commitments to consumers, different competition environments and different abilities to solve problems. If we adopt a uniform regulatory approach to the entire internet, we are going to be left with the lowest common denominator, something like transparency with enforcement that just prohibits deceptive practices. And that is not good enough. Consumers are asking for more.

I appreciate your commitment to this issue. Thanks for having me. I look forward to answering your questions.

[The prepared statement of Ms. Moy follows:]



Statement of Laura Moy, Deputy Director
Center on Privacy & Technology at Georgetown Law

Before the

U.S. House of Representatives

Committee on Energy and Commerce

Subcommittee on Communications and Technology

Hearing on

Protecting Customer Proprietary Network Information in the Internet Age

Wednesday, July 11, 2018

For more information, contact Laura Moy at laura.moy@georgetown.edu.

Introduction and Summary

Chairman Blackburn, Ranking Member Doyle, and Members of the Subcommittee:

Consumers feel that they have lost control of their private information, and consistently are asking for greater control. 91% of adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies, and 68% believe current laws are not good enough in protecting people's privacy online.

Today's hearing is framed around customer proprietary network information, or CPNI. Generally speaking, CPNI is information collected by telecommunications providers about subscribers' use of the service. Information like who we call, and who calls us; how often we call them; how long we talk to them; and where we're calling from.

It is appropriate for a hearing about privacy to be framed around CPNI because the law that protects CPNI is one of the strongest federal consumer privacy laws we have.[1] It requires that phone carriers get their customers' consent before using CPNI for purposes other than to provide the phone service. In other words, phone carriers simply deliver the service we pay for without always trying to make an extra buck off of the details of our private lives. That means that a phone carrier cannot use the fact that a customer has been calling banks and credit card companies to market him payday loans, or that a customer has been calling an elderly relative and doctors' offices more frequently to market her home health services. Nor can it sell that information to outsiders—not without getting the customer's permission.

The CPNI privacy law also allows an expert agency to craft specific rules implementing the statute—rules that can be modified and updated in accordance with changing technology and business practices. For example, FCC rules protecting CPNI require phone carriers to protect customers' call details with a customer-created PIN, to maintain records of all sales and marketing campaigns that use their customers' CPNI, and to notify customers of security breaches.

The CPNI privacy law also gives the FCC robust enforcement authority in the form of fines. Using this authority, just in the last few years the FCC:

---

[1] 47 U.S.C. § 222.

- Slapped Verizon with fines when the company misused its customers' private information for internal marketing;
- Fined smaller providers YourTel and TerraCom for storing customers' sensitive information on unprotected Internet servers that anyone could access; and
- Fined AT&T $25 million when call center employees who were working with people trafficking in stolen cell phones accessed customer records without authorization.

The CPNI privacy law should serve as a model for future privacy laws this Congress may consider, because of its substantive strength, the regulatory flexibility it offers through rulemaking, and its enforcement strength.

Instead, however, the benefits to consumer privacy presented by the CPNI privacy law have faced major setbacks. Last year Congress—including a number of members of this subcommittee—voted against the extension of these strong CPNI privacy rules to broadband providers. Like the phone, broadband is now an essential service. And like phone carriers, broadband providers enjoy privileged insight into their subscribers' private communications. This year, as it eliminated net neutrality rules, the FCC removed broadband providers altogether from the reach of the CPNI privacy law—which, as I said, might be the strongest consumer privacy law we have on the books.

That brings us to today, and here, as we consider what our path forward should be. Consumers clearly want *more* privacy protection, not *less*—this is why the recent elimination of existing privacy protections was so unpopular among the American public.[2] As Congress considers how to give Americans the privacy protections they deserve, it should keep a few things in mind:

- Rulemaking authority is needed to protect consumer privacy prospectively and foster regulatory flexibility.
- Consumer protections are only as good as their enforcement, so any new protections Congress creates on privacy or data security must

---

[2] *See* Matthew Yglesias, *Republicans' Rollback of Broadband Privacy Is Hideously Unpopular*, Vox (Apr. 4, 2017), https://www.vox.com/policy-and-politics/2017/4/4/15167544/broadband-privacy-poll.

be accompanied by strong enforcement, including civil penalty authority.

- Congress should avoid the temptation to address complex challenges with a one-size-fits-all approach.
- Congress should not eliminate existing protections for consumers' information.

I appreciate your commitment to this issue.

1. Online privacy is important

Consumers care about and have well-founded concerns about online privacy. In response to one 2015 survey, 80% of respondents were "concerned" or "very concerned" when asked about their online privacy.[3] For years, consumers have been expressing concern and even anger about the way their personal information is collected and used without their control, consent, or even knowledge.[4] Consumers feel powerless to regain control over their privacy—in the modern era, Internet access is necessary for employment, education, access to housing, and full participation in economic and civic life.

Consumer privacy concerns can chill both adoption and free and open use of the internet. For example, according to an FCC survey in 2010, 57% of Internet non-adopters reported feeling that online activities made it too easy for theft of personal information.[5] The FCC concluded in the *National*

---

[3] Freedman Consulting, *Poll Finds Strong Support for Expanding Online Privacy Protections and Internet Access* (Nov. 23, 2015), *available at* https://www.freedmanconsulting.com/documents/PrivacyandAccessResearchFindings_151123.pdf.

[4] Lee Rainie & Maeve Duggan, Pew Research Center, *Privacy and Information Sharing* 2 (Jan. 14, 2016), http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf ("In online focus groups and in open-ended responses to a nationally representative online survey, many people expressed concerns about the safety and security of their personal data in light of numerous high-profile data breaches. They also regularly expressed anger about the barrage of unsolicited emails, phone calls, customized ads or other contacts that inevitably arises when they elect to share some information about themselves.").

[5] This number was reported in contrast to 39% of adopters who felt the same way. John Horrigan, *Broadband Adoption and Use in America* 17 (FCC Nat'l Broadband Plan, Working Paper No. 1, 2010),

Broadband Plan that concerns about online privacy and security "may limit [consumers'] adoption or use of broadband."[6] More recently, NTIA reported that 45% of households limited their online activities because of privacy and security concerns.[7] And in 2016, focus groups examining adoption challenges in Portland, Oregon universally raised privacy concerns.[8]

It is particularly important to protect online privacy because the Internet is where we practice First Amendment speech in the modern era. The health of our democracy relies on the Internet functioning as a trustworthy platform for free and unfettered association and speech. But as privacy diminishes, so does speech. For example, studies have shown that people self-censor opinions they believe may be unpopular when informed that they are under surveillance.[9]

2. Protections for consumers' private information should be forward-looking and flexible

To foster the increased control over private information that consumers want, Congress should consider establishing protections that are forward-looking and flexible. Agencies that are to be tasked with protecting consumers' private information should be given rulemaking authority, just as the CPNI statute grants rulemaking authority to the FCC. After-the-fact enforcement can be helpful, but an enforcement-only regime does not always

---

https://transition.fcc.gov/DiversityFAC/032410/consumer-survey-horrigan.pdf.

[6] FCC, *Connecting America: The National Broadband Plan* 17 (2010), https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.

[7] Rafi Goldberg, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities, NTIA (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[8] Angela Siefer, Signs On Letter Encouraging FCC Protect Privacy Of Broadband Consumers, NDIA (Jan. 26, 2016), http://www.digitalinclusionalliance.org/blog/2016/1/26/ndia-signs-on-letter-encouraging-fcc-protect-privacy-of-broadband-consumers.

[9] *See* Elizabeth Stoycheff, Mass Surveillance Chills Online Speech Even When People Have "Nothing to Hide," Slate (May 3, 2016), http://www.slate.com/blogs/future_tense/2016/05/03/mass_surveillance_chills_online_speech_even_when_people_have_nothing_to.html.

create clarity, and because it comes only after a problem has occurred, it does not necessarily protect consumers from the problem in the first place.

In particular, the FTC should be given rulemaking authority over data security, data brokers, and consumer privacy. The FTC brings the bulk of federal privacy enforcement actions, but it only has after-the-fact enforcement authority, with no ability to define rules of the road before consumer data is used in ways that consumers consider inappropriate. And with few exceptions, when it comes to privacy and data security the FTC can only take enforcement action against entities that use consumer information in ways that violate their own consumer-facing commitments. Indeed, commissioners of the agency have themselves asked Congress for rulemaking authority.[10]

Rulemaking authority helps to future-proof consumer protections, enabling agencies to adjust regulations as technology changes, as the FTC did just a few years ago with the COPPA Rule.[11] Consumers are constantly encountering new types of privacy and data security threats as the information landscape evolves. Where flexibility exists, policymakers use it to respond to changing threats. For example, states adjust data security and breach notification protections as changing circumstances require, such as by extending protection to additional categories of information, including medical information and biometric data.[12] We can't always forecast the next

---

[10] Maureen K. Ohlhausen, FTC Commissioner, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), *available at* https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf ("Legislation in both areas – data security and breach notification – should give the FTC the ability to seek civil penalties to help deter unlawful conduct, rulemaking authority under the Administrative Procedure Act, and jurisdiction over non-profits.");

[11] Federal Trade Commission, *FTC Strengthens Kids' Privacy, Gives Parents Greater Control over Their Information by Amending Children's Online Privacy Protection Rule* (Dec. 19, 2012), https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.

[12] William Elser, *Recent Updates to State Data Breach Notification Laws in New Mexico, Tennessee, Virginia*, Lexology (May 1, 2017), https://www.lexology.com/library/detail.aspx?g=b02a15ac-a3c3-460d-bc5e-1d29778c4e59 ("New Mexico's new law defines 'personal identifiable information' consistently with most other states, and joins a growing number of states that have broadened the definition to include 'biometric data,' which is

big threat years in advance, but unfortunately, we know that there will be one.

The law should grant an expert agency or agencies the authority to develop prospective privacy and data security rules, in consultation with the public, so that data collectors and users can know in advance what standards apply to consumers' information.

3. Protections for consumers' private information should be strongly enforced

Congress also should ensure that whatever agency or agencies are to be in charge of enforcing privacy and data security standards have substantial civil penalty enforcement authority, just as the CPNI statute grants the FCC. Regulations are effective to deter violations only if entities fear the punishment that would surely follow.

Agencies recognize the importance of—and ask for—strong enforcement tools. Indeed, the FTC has repeatedly asked for the civil penalty authority it needs to enforce data security.[13] At present when the FTC takes action to enforce, it is generally unable to pursue penalties that would serve as an effective punishment for violators, and an effective deterrent for others.[14] To improve privacy and data security for consumers, the FTC—or

---

defined to include 'fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry.'").

[13] *See, e.g.*, Testimony of Jessica Rich, Federal Trade Commission, before the House Oversight and Government Reform Committee Subcommittees on Information Technology and Health, Benefits, and Administrative Rules regarding Opportunites and Challenges in Advancing Health Information Technology (Mar. 22, 2016) at 7, *available at* https://oversight.house.gov/wp-content/uploads/2016/03/2016-03-22-Rich-Testimony-FTC.pdf; Maureen Ohlhausen, Commissioner, Fed. Trade Comm'n, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), transcript *available at* https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf.

[14] There are exceptions to this rule. As the FTC explains, "If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales

another agency or agencies—must be given more powerful regulatory tools and stronger enforcement authority.

Agencies also need resources to do their jobs well. Unlike the FCC, the FTC has no Office of Engineering & Technology. An agency expected to enforce the privacy and security obligations of companies that do business in a digital world should be vested with the necessary expertise and resources to do that job well.

To provide an additional backstop for consumers the event that agencies lack the capacity or motivation to effectively enforce, Congress should also consider granting state attorneys general or even individual consumers themselves the right to bring civil actions against companies for violating privacy regulations. This type of authority exists, for example, under the Children's Online Privacy Protection Act.[15]

4. Protections for consumers' private information should take into account the context in which information is shared

There is no one-size-fits-all approach for privacy. Rather, privacy laws and regulations should be context-specific, carefully tailored based on the avoidability of the information sharing, the sensitivity of the information shared, and the expectations of consumers.

When information sharing is unavoidable or less avoidable by consumers, it is important that heightened privacy protections apply. This explains in part why there are a variety of laws that protect consumer information in specific contexts in which sharing is unavoidable—such as the information shared by students in an educational context,[16] by consumers in a financial context,[17] by customers in a telecommunications context,[18] and by patients in a medical context.[19]

Rule." FTC, *Privacy & Security Update 2016*, https://www.ftc.gov/reports/privacy-data-security-update-2016.

[15] For example, the Children's Online Privacy Protection Act enables state attorneys general to bring actions on behalf of residents of their states against operators of online sites or services that they believe have violated children's privacy regulations. 15 U.S.C. §6504.

[16] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

[17] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).

[18] 47 U.S.C. § 222.

[19] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).

This is also consistent with the FTC's evaluation of potentially problematic data-related practices under its Section 5 authority to prohibit unfair practices. When considering whether a practice is unfair, the FTC asks not only whether the practice is harmful, but also whether the practice is one that consumers can avoid. In its policy statement on unfairness, the FTC explained,

> Normally we expect the marketplace to be self-correcting, and we rely on consumer choice—the ability of individual consumers to make their own private purchasing decisions without regulatory intervention—to govern the market. We anticipate that consumers will survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory. However, it has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary. Most of the Commission's unfairness matters are brought under these circumstances. They are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking.[20]

In recognition of the heightened privacy protections that should attach to information consumers cannot avoid sharing, Congress should consider strengthening the FTC's unfairness authority.

Whether or not information sharing is avoidable by a consumer is often tied to the question of whether or not a service or transaction is essential. When a service is essential—such as with phone service—information sharing may be considered unavoidable because the consumer cannot reasonably decline the service altogether. This, too, helps explain why heightened privacy protections apply in the educational,[21] financial,[22]

---

[20] FTC, *FTC Policy Statement on Unfairness* (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
[21] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
[22] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).

telecommunications,[23] and medical contexts—all of these contexts involve essential services.[24]

In determining what level of protection should be afforded to information shared in a particular context, policymakers should also examine how sensitive the shared information is. For example, the Children's Online Privacy Protection Act recognizes that information about children deserves heightened protection.[25] Other laws recognize the heightened sensitivity of health information[26] and financial information.[27] In the past, the question of sensitivity has often been the most important in considering how well the law should protect consumers' information. Data analysis techniques have advanced over time, however, and it is becoming clear that classically sensitive information can often be deduced from categories of information not traditionally thought of as sensitive. For example, as computer scientist Ed Felten explained in testimony before the Senate Judiciary Committee regarding telephone metadata, "Calling patterns can reveal when we are awake and asleep; our religion . . . our work habits and our social attitudes; the number of friends we have; and even our civil and political affiliations."[28] In 2016 the FTC found that television viewing history can be considered sensitive information,[29] and the Federal Communications Commission (FCC) found that web browsing history can be considered sensitive.[30] Indeed, patent

---

[23] 47 U.S.C. § 222.
[24] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).
[25] 15 U.S.C. §§ 6501–6506.
[26] *E.g.* Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).
[27] *E.g.* Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).
[28] *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing before the S. Comm. on the Judiciary,* 113th Cong. 8-10 (2013) (statement of Edward Felten, Professor of Computer Science and Public Affairs, Princeton University) *available at* http://www.judiciary.senate.gov/meetings/continued-oversight-of-the-foreign-intelligence-surveillance-act.
[29] Complaint at ¶ 32, *FTC v. Vizio*, Case No. 2:17-cv-00758, D.N.J. (filed Feb. 6, 2017), *available at* https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.
[30] Federal Communications Commission, *Fact Sheet: The FCC Adopts Order to Give Broadband Consumers Increased Choice over Their Personal Information*, https://apps.fcc.gov/edocs_public/attachmatch/DOC-341938A1.pdf.

applications filed by Google indicate that it is possible to estimate user demographics and location information based on browsing histories.[31]

Protection for consumers' information should also be tailored based on consumers' expectations for how the information will be used.

5. Congress should not eliminate existing protections for consumers' information

Perhaps this should go without saying, but as Congress considers establishing new privacy and data security protections for consumers' private information, it should not eliminate existing protections. Americans are asking for *more* protections for their private information, not less. This explains why when this body voted last year to eliminate strong privacy regulations that had recently been passed by the FCC, consumers—on both sides of the aisle—were outraged.[32] Some lawmakers argued that repeal of the FCC's rules was needed to foster development of a consistent approach to privacy across the Internet.[33] But as FTC Commissioner Terrell McSweeny noted, "If consistency were truly the goal, then we would likely increase protections for privacy, rather than unraveling them. That is the policy conversation we ought to be having—instead we are fighting a rear-guard action defending basic protections."[34]

---

[31] *See* U.S. Patent Application No. 13/652,198, Publication No. 20130138506 (published May 30, 2013)(Google Inc., applicant)("demographics data may include a user's age, gender, race, ethnicity, employment status, education level, income, mobility, familial status (e.g., married, single and never married, single and divorced, etc.), household size, hobbies, interests, location, religion, political leanings, or any other characteristic describing a user or a user's beliefs or interests."); U.S. Patent Application No. 14/316,569, Publication No. 20140310268 (published Oct. 16, 2014)(Google Inc., applicant).

[32] *See* Matthew Yglesias, *Republicans' Rollback of Broadband Privacy Is Hideously Unpopular*, Vox (Apr. 4, 2017), https://www.vox.com/policy-and-politics/2017/4/4/15167544/broadband-privacy-poll.

[33] *See* Alex Byers, *House Votes to Revoke Broadband Privacy Rules*, Politico (Mar. 28, 2017), https://www.politico.com/story/2017/03/house-votes-to-revoke-broadband-privacy-rules-236607.

[34] Terrell McSweeny, Commissioner, Fed. Trade Comm'n, Remarks on *"The Future of Broadband Privacy and the Open Internet: Who Will Protect Consumers?"* (Apr. 17, 2014), at 4, https://www.ftc.gov/system/files/

Congress also should not eliminate existing and future consumer protections at the state level. State laws play an important role in filling gaps that exist in federal legislation, and state attorneys general play an important role in enforcing privacy and data security standards.[35] For example, in data security and breach notification, some state laws protect categories of information that are not protected by other states, and would not be protected by a number of proposals for federal data security and breach notification legislation.[36] State attorneys general play a critical role in policing data security and guiding breach notification to match the needs of their own residents, and are essential in conducting ongoing monitoring after a breach has occurred to help protect residents from any aftermath, especially where small data breaches are concerned. According to the Massachusetts State Attorney General's Office, Massachusetts alone saw 2,314 data breaches reported in 2013, 97% of which involved fewer than 10,000 affected individuals.[37] Each data breach affected, on average, 74 individuals.[38]

6. Conclusion

I am grateful for the Subcommittee's attention to these important issues, and for the opportunity to present this testimony.

---

documents/public_statements/1210663/mcsweeny_-_new_americas_open_technology_institute_4-17-17.pdf.

[35] *See generally* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747 (2016).

[36] *See* Testimony of Laura Moy before the House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade regarding the Data Security and Breach Notification Act of 2015 (Mar. 11, 2015) at 3–5, *available at* https://democrats-energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony-Moy-CMT-Data-Breach-Legislation-2015-03-18.pdf; *see also* Responses to Additional Questions for the Record of Laura Moy before the House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade, http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-MoyL-20150318.pdf.

[37] Testimony of Sara Cable before the House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade regarding the Data Security and Breach Notification Act of 2015, *available at* http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-CableS-20150318.pdf.

[38] *Id.*

Mrs. BLACKBURN. The gentlelady yields back.

And we thank all of you for your testimony. And we will begin our questions and answers. I will begin by recognizing myself for 5 minutes.

Mr. Haney, I would like to start with you. Devices often have much more detail location information than what carrier location provides. For example, later iPhone models integrated location information from various sensors, Wi-Fi, Bluetooth, GPS, cell towers, et cetera, and create a more precise location. Apple calls this data Hybridized Emergency Location, or HELO. Is this feature integrated into the operating system?

Mr. HANEY. Yes, I believe it is.

Mrs. BLACKBURN. And would you classify HELO data as CPNI?

Mr. HANEY. No.

Mrs. BLACKBURN. If you applied current CPNI rules to HELO data, would Apple be permitted to transfer this data to a service like RapidSOS?

Mr. HANEY. No, not without subsequent permissions.

Mrs. BLACKBURN. OK. Would Uber, which relies on HELO data, be able to function if HELO data was subject to CPNI rules, or would the app become unusable due to individual opt-in consent mechanisms every single time a user opens the app?

Mr. HANEY. In terms of ability to function, no, probably not. In terms of the consumers, they probably suffer from opt-in fatigue.

Mrs. BLACKBURN. OK. Thank you.

Mr. McDowell, how is the data that is collected by mobile apps different from the data collected by a telecom provider? Because it does not sound that different to me. Mobile apps are collecting the time an app is used, the duration, and the location of where the user is when they are using the app. And we heard through our algorithms hearing that we recently did how all this collection goes even a step further and anticipates my future choices, plans, and decisions.

So aren't these the same details a telecom provider collects and are protected under the CPNI rules? And what are the rules protecting this information from a mobile app, and what level of opt-in has the consumer performed?

Mr. MCDOWELL. A lot of questions there, Madam Chair.

Mrs. BLACKBURN. Yes.

Mr. MCDOWELL. All excellent ones. So, first of all, an app can actually collect more data than a carrier would have access to. For instance, if you scan a UPC code, the price of something in a supermarket, there is an app that can tell you if there is a better deal nearby. So it knows where you are, it knows what you are buying, it knows your price points. It knows a lot about you all of a sudden, the demographics, based on that thing that you are buying. That is just one of many examples.

It is the 10th anniversary this week of the Apple App Store. So happy birthday to the App Store. I think it is a wonderful thing. And there are, I think, 1.5 million apps in that app store. And certainly, Apple has some terrific standards that it tries to live by there. But those apps, with 1.5 million, or whatever the actual number is, there are just as many ways of gleaning information about consumers, where they are, what they are buying, what they

want, what they are saying, how they look. There are a lot of aspects there that carriers don't necessarily have access to.

So the CPNI rules would be sort of a—or the data that CPNI governs would be sort of a subset of what all the other information that apps collect.

Mrs. BLACKBURN. You mentioned we need to modernize and harmonize the protection rules. So I want you to elaborate just a touch on that point.

Mr. MCDOWELL. Absolutely. So from a consumer's perspective, there is certain information that we find sensitive. And this can vary from consumer to consumer, of course, and other information not. So if you think of your information regarding your health or your financial information, things like that, those are easy examples of what we consider to be sensitive, and you don't necessarily want the whole world, or very few people, having access to that, versus you are conducting a search to buy a new car. Maybe you want to have the greater world know that you are looking for this kind of car at this type of price point. So that is less sensitive information.

So that is what I was trying to illustrate too, is as consumers, we care about the type of information. It doesn't matter who has that information. There aren't politically favored or politically disfavored entities out there. We are concerned about anyone breaching that or disclosing that information in a way that we don't agree with or the way that we don't command.

Mrs. BLACKBURN. OK. I appreciate that.

Ms. Moy, I have a question for you. In the interest of time, I will submit that.

I yield back my time and recognize Mr. Doyle.

Mr. DOYLE. Thank you, Madam Chair.

Ms. Moy, it was recently revealed that our nation's top wireless carrier shared real-time location data of hundreds of millions of Americans with third parties without consumers' consent. This access was used by at least one entity, Securus, as part of a service to enable their customers to determine the exact location of hundreds of millions of cell phones in real time without user consent.

How is it possible that such a massive data breach of such sensitive data could occur, and why do you think the FCC was in the dark on such a widespread practice?

Ms. MOY. Those are really good questions, and questions that the agency itself should be asking. So in this instance, Securus was getting information through these data brokers, location aggregators, that were sourcing it directly from the wireless carriers who were giving these data brokers direct access into their location information.

We know about the Securus case, but about a month ago, Verizon told journalist Frank Bajak of the Associated Press, that about 75 companies have been obtaining its customer data from LocationSmart, and another broker called Zumigo, I think. And I want to emphasize that this is really private information. Location can tell someone about where you work, where you live, where your kids go to school. In a recent Supreme Court decision, the Court likened location data maintained by phone carriers to electronic ankle bracelets.

With respect to how this could have happened, clearly, the carriers have not been taking location privacy seriously enough, if they were enabling data brokers to take over the customer consent process and then not properly policing it. But ultimately, the responsibility falls with the FCC to ensure that carriers are actually meeting their statutory obligation to protect that information.

Mr. DOYLE. So tell me, if a Federal regulator is captured by industry and declines to assert their own authority, what role does the private right of action or enforcement authority by state attorney generals play, and how can that maybe be a check on a reluctant agency?

Ms. MOY. That is a great question, because we have something sort of like that under the—well, we do have that under the Children's Online Privacy Protection Act. The Children's Online Privacy Protection Act, which is a 1998 privacy law that specifically involves the information that children share with a provider of an online site or service, grants state attorneys general the authority to bring civil actions against companies that they believe have violated the Act—or have violated, actually, the regulations passed by the FTC under that act on behalf of citizens of the state in the event that the agency itself, the Federal agency, doesn't do that.

I think that is a really important and strong privacy enforcement tool. It has been used by multiple state attorneys general, and it would be great to see something like that in additional privacy laws moving forward.

Mr. DOYLE. Tell me, do you think Chairman Pai's past work for Securus is reason for him to recuse himself from any investigation or enforcement action?

Ms. MOY. I don't know that I can answer that directly, except to say that I do; it does raise some red flags that he does have a past working for a company that is accused of wrongdoing in this particular instance.

Mr. DOYLE. Let me ask you, do you think Americans have fewer privacy protections as a result of the broadband privacy CRA?

Ms. MOY. As a person who advocated strongly for those broadband privacy rules and thinks that they are really important, yes, I do. I think that privacy is in a worse place, especially when you think about your home internet connection. An internet provider can see not only information about all of the websites that you visit, including those that pertain to your health information, your political viewpoints and so on, but can also see information about Internet-of-Things connected devices. So perhaps information about when you are opening your garage door, when you are using your baby monitor, maybe even when you are using your connected toothbrush or connected mattress. They can see maybe when there are guests in your home and additional devices. There is just a lot of really sensitive information that a network provider has access to, and consumers, unfortunately, have no choice but to share that information with those providers.

Mr. DOYLE. Do you think Americans are better off with the FTC enforcing privacy protections on broadband providers as some in the majority have alleged?

Ms. MOY. Frankly, no. There are multiple reasons, but part of it is that the FTC doesn't have rulemaking authority, so it can't cre-

ate perspective rules-of-the-road on this issue. And its enforcement tools are really limited. It doesn't have the same kind of bite to its enforcement that the FCC does.

As I said, the FCC has brought multiple actions against carriers in the past few years for CPNI violations with fines attached. The FTC doesn't have that type of authority.

Mr. DOYLE. Thank you, Madam Chair. I yield back.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Olson, you are recognized for 5 minutes.

Mr. OLSON. I thank the chair. And welcome, Mr. Haney, Ms. Moy. And a special welcome to the McDowell family, our commissioner, and his daughter Mary-Shea is right behind his left shoulder.

We talked before the hearing. She is a junior in high school, about to go off to college, and I take great pride, as your father does as well having—my wife went to Duke University like your father. You won't become a North Carolina Tar Heel. Never, ever. So thank you for that.

But to the business ahead, Commissioner McDowell, we have all become familiar with the idea of targeted advertising. As you know, companies grab our data and, when we buy something—like, for example, I bought a lot of Houston Astros World Series hats, Jose Altuve jerseys, George Springer bobblehead. All of a sudden, ads popped up, when I got on the internet, with the Astros, the Rockets, the Oilers, pro-baseball. Obviously, they are targeting me with direct ads because of my behavior on the internet.

Google and Facebook as well do this automatically. Users like myself have to opt out most times, because I don't want those targeted ads. Most people don't want those ads. But if a telecommunications provider does this automatically, the exact same behavior that Googles and Facebooks do, that is illegal.

Can you explain that? Doesn't that sound anticompetitive?

Mr. MCDOWELL. Well, it does create that asymmetry that I was talking about in my opening remarks. So that is because of section 222 and the FCC's enforcement of that. So we have a diverse internet ecosphere. There are business models that have come forth in the past decade, even the past year or two, that we couldn't even imagine a year or two ago, right. So we don't know what is coming up next, what brilliant entrepreneurs are going to think of.

So we don't know ways they might be using our data. But you do have 222, section 222, offering one standard and FTC sometimes administering a different standard.

Mr. OLSON. Mr. Haney, in your opening statement, you state that "privacy protection encourages broadband usage and therefore promotes broadband investment." So this should incentivize broadband providers to invest heavily in privacy protection.

Is this what you see in the marketplace? Does it work in the market?

Mr. HANEY. I think in the marketplace, privacy protection can be strengthened, but I think that current privacy protection is working in the market to incentivize all providers to invest, to create for consumers more abundance of choices, lower prices, services that we can't even imagine at this point. And I think that to the extent that Congress through legislation enhances consumer pri-

vacy, that it is very important, not only to be certain that all providers are created equally, but also that the privacy regulation is not overly burdensome.

Mr. OLSON. Thank you.

Back to you, Commissioner McDowell, about my Houston Astros hats purchases swarm me with ads. Most consumers, as we mentioned, don't want their call detail information released to third parties or used for targeted ads. It doesn't matter if that call comes from a digital telephone or even an app.

Do you believe the best way to address this problem would be with one technology neutral privacy rule that covers all call detail information?

Mr. MCDOWELL. I think one standard would be very helpful and would allay a lot of confusion among consumers and market players of all kinds alike.

So when I was at the Commission in 2007, we expanded the CPNI rules to what we call interconnected Voice over Internet Protocol providers, or interconnected VoIP, as we call it. But if you are not an interconnected VoIP, if you are just VoIP, using internet protocol through an app, then it is not regulated by 222. But to the consumer, it is the same function. It is an internet voice and video call to someone.

One type, if it is interconnected, is regulated in 222. Another type, if it is not interconnected to the PSTN, the public switched telephone network, is not. So that creates that asymmetry and a lot of confusion for folks, I think.

Mr. OLSON. Well, thank you. I will close with a comment on Hurricane Harvey. During your tenure at the FCC, you were pushing hard after hurricane Ike hit my hometown about putting your lines below the soil, bury them. We did that for Harvey. Those lines stayed up the whole time. Information critical for emergency were being flown all across Houston areas. So thank you, thank you for that.

Go Blue Devils. Beat the Tar Heels forever.

I yield back.

Mr. MCDOWELL. I did not ask him to say that.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Pallone, you are recognized for 5 minutes.

Mr. PALLONE. Thank you, Madam Chair.

Today's hearing highlights how much consumers on the internet have lost over the past year and a half. Consumers' privacy protections, consumers' data security protections, and consumers' net neutrality have been ripped away. So I think it is a rough time to be online.

The Republicans delivered a one-two punch when they rolled back consumer broadband privacy rules and then repealed the net neutrality safeguards that ensure the internet remain free and open.

So let me start, Ms. Moy, can you explain how these two anti-consumer actions worked in concert to give consumers fewer privacy protections online?

Ms. MOY. Sure. Yes. So the first was these set of rules that really implemented section 222, the CPNI law, which, as I said, is one of the strongest consumer privacy laws that we have, and apply it to

broadband providers. And unfortunately, Congress undid those regulations with the CRA resolution.

But even after the CRA resolution, section 222, at least the statute of it, still applied to broadband providers until the more recent net neutrality order that undid the net neutrality rules, as well as Title II classification.

So consumers now are left without the statutory protections of 222 to apply to broadband information and are left only with the baseline prohibition on unfair and deceptive practices under section 5 of the FTC Act, which more or less just prohibits broadband providers from doing things other than what they have told consumers in a consumer-facing statement they would do.

Mr. PALLONE. Well, thanks.

Let me ask Mr. Haney. It is evident that in the internet age, so many different entities have access to our private information. And you also make mention of this in your written testimony. So if you could tell me, what types of companies, other than phone companies, have access to information traditionally thought of as CPNI, and are they subject to as stringent regulations as telecommunications companies?

Mr. HANEY. I mention video streaming services, search engines, social networking sites, e-commerce sites, and user-generated media sites as examples. And currently, they are subject to the same privacy regulation as broadband providers, but as I mentioned, broadband is not the same thing as a common carrier telecommunications service. And therefore, only the common carrier telecommunications service, what we think of as telephone calls or any voice communication, excepting a voice app that is not interconnected to the public switched telephone network, that would be the only category that would be subject to the privacy protection that Ms. Moy supports.

Mr. PALLONE. All right. Thank you.

Let me go back to Ms. Moy. I was alarmed by the reports of the vast troves of location data that third-party aggregator LocationSmart was making available to anyone on the web. It seems to me that we don't even know yet the entire scope of that incident. So do we know how exactly and how many companies or individuals have access to the data that LocationSmart was making available and what these data were used for?

Ms. MOY. We don't know. We know the one specific example of Securus, we know that in some detail because there were public records posted on the Georgia Department of Corrections website that showed screen shots from what the Securus platform looked like. And alarmingly, it enabled users of that platform to enter in the phone number of any phone in the country, upload a document of any sort, and without that document being scrutinized, they could obtain real-time location information for any individual in the country.

We do know, as I said before, from an AP report that 75 companies reportedly had access to location information through LocationSmart pertaining to Verizon customers. But I think it is safe to say that this is just the tip of the iceberg, right? If all four major wireless carriers were outsourcing a location information access to these third-party data brokers, only one of which is

LocationSmart, then we are probably just seeing the very beginnings of what could be a massive investigation and a lot of privacy violations.

Mr. PALLONE. Do you have any suggestions what the FCC could do to help us better understand the scope of this incident problem?

Ms. MOY. So the CPNI rules do require carriers to maintain records about who has access to customer CPNI, using the customer consent model. And so the FCC ought to be able to, using its investigatory authority, ought to be able to demand those records from the major wireless carriers, and that trail of records should lead them right down the path to finding out how many violations there were. And if those records don't exist, then that is a violation in and of itself.

Mr. PALLONE. Thank you. Thank you, Madam Chair.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Lance, you are recognized for 5 minutes.

Mr. LANCE. Thank you very much. And I apologize to the panel for shuttling. We have several subcommittees this morning. This is a very important topic, and certainly we want to proceed in a bipartisan way on it.

Given the rules implementing 222 continue to distinguish between local and long distance service and impose authentication requirements that are 20 years and perhaps out of date, do you believe that the current rules make sense in today's modern marketplace or do you believe that we should update them reflecting consumers' current expectations?

And this is for the panel in its entity. Mr. Haney?

Mr. HANEY. I believe the rules, sir, are out of date. They were designed, not only to protect consumer expectations, but they were also designed to try to allocate competitive advantages and competitive disadvantages in the marketplace as new entrants joined the market to compete with traditional incumbents. That dynamic is no longer relevant, and so I believe that the rules can and should be updated. But I do think it is important, sir, that the rules should apply equally to everyone. Every provider in the internet ecosystem is in a position to see and to collect information about consumers, some of it sensitive.

Mr. LANCE. Mr. McDowell.

Mr. MCDOWELL. I would agree with Mr. Haney in that the rules are out of date. Twenty two years ago was when Congress passed section 222. Every aspect of the internet ecosphere is completely different now than it was then in terms of data collection as well.

And one also point to follow up on the exchange with Mr. Pallone, is that, if you have a device, like Mary-Shea's little brother Cormac, he has a hand-me-down iPhone, but he is not a subscriber, so he lives off the land, so to speak, through unlicensed. And those transmissions—voice, video, apps, gaming, whatever—would not be covered, right, except by the FTC. They are not covered under 222.

So this starts to talk about the limitations or point out the limitations, and there are millions of nonsubscribers such as our youngest child, Cormac.

Mr. LANCE. Thank you.

Ms. Moy.

Ms. MOY. Thank you. So the regulations almost were updated, as you know, and the updates to those regulations would have applied to phone providers who are subject to the CPNI rules as well as to broadband providers to whom the CPNI rules had been extended. And so that included, for example, an update of the data security provisions in the CPNI rules to do away with some of the more prescriptive things that was maybe an older approach to data security and to replace it with a more flexible, reasonable security measures standard in accordance with several factors, such as the nature and scope of the carrier's activities, the sensitivity of the data that it collects, and so on.

So I do believe that updates to the rules such as those that were almost enacted that were passed in 2016 and then reversed by the CRA resolution would be appropriate. And the question is just how we get back to where we are.

Mr. LANCE. Would they have applied across-the-board?

Ms. MOY. They would have applied to phone carriers as well as to broadband providers. If you are asking if they would have applied to other entities such as apps and so on, no, they would not. And I would completely support rulemaking authority to apply similar regulations to——

Mr. LANCE. I am a co-sponsor of the chairman's legislation, the BROWSER legislation, and I would hope that the distinguished panel would look at it. And the chairman has taken the lead across this country in this area, and I am pleased to associate myself with what the chairman is attempting to do here. And I certainly agree with the panel that we need to update the procedures.

Mr. McDowell, if Congress enacts new privacy legislation, should information about calls be treated the same regardless of how a call is made?

Mr. MCDOWELL. If Congress looks at this, yes, again, back to one uniform standard, I think that that would be very helpful to everybody involved. As we are finding out today, it is a complicated issue. It doesn't need to be as complicated.

Mr. LANCE. Thank you. And, Chairman, I yield back 32 seconds.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Welch, you are recognized.

Mr. WELCH. Thank you very much.

Mr. Haney, do you believe that the CPNI rules as they apply to telecoms have served a good function to protect privacy of telephone users?

Mr. HANEY. I think the rules were more onerous than they needed to be, but——

Mr. WELCH. Well, go ahead.

Mr. HANEY. I think that the requirement to get opt-in consent actually inhibited innovation, because as it applied to the incumbents in the marketplace, it is very difficult to get opt-in consent from consumers.

Mr. WELCH. All right. I am going to come back to that. Do you think that the privacy protections, though, that were outlined in the CPNI did ultimately protect privacy rights of the users?

Mr. HANEY. Yes, sir.

Mr. WELCH. And would you have a problem having that privacy protection applied across all technologies?

Mr. HANEY. I think if it applied across all technologies, it would be a huge improvement.

Mr. WELCH. So CPNI across all technologies you would be supportive of?

Mr. HANEY. Well, except for the fact that I do believe it is overly burdensome.

Mr. WELCH. All right. I am going to try to summarize what I am hearing. Because, number one, all three of you, I think, want technology-neutral provisions, correct? And I don't think there is opposition up here to having it be technology neutral.

Number two, you want a uniform enforcement so it is not complicated, right?

Mr. HANEY. Yes.

Mr. WELCH. So, three, there is a big debate about this opt in or opt out. And essentially, that is the burden. Who is going to be protected? Is it going to be the consumer and he or she has the opportunity to opt in or opt out versus the burden that the opportunity costs for the technology provider.

Isn't that essentially what it boils down to?

Mr. MCDOWELL. If I could add to that, yes. So certainly, and earlier what Mr. Haney said, there is the potential for opt-in fatigue, as we see with the GDPR in Europe. I don't think that is the standard we want to operate on. I think that would actually suffocate our internet ecosphere, but——

Mr. WELCH. Let me——

Mr. MCDOWELL. But uniformity, that concept, I think——

Mr. WELCH. But here is the thing. I am a consumer. I don't have a clue how all these things operate, and that is how most of us are. I would feel much more comfortable if I was able to opt in or not. If it was the opt-in approach, I would feel more empowered.

Mr. MCDOWELL. Coming over the horizon too real quick—sorry—we ought to probably have another hearing some day on blockchain and the evolution of blockchain and how that is going to help privacy protection. That is a whole other technological argument——

Mr. WELCH. You know what, I actually got to say I don't buy that.

Mr. MCDOWELL. OK.

Mr. WELCH. And here is why. There is always something over the horizon. All right. None of us have a clue as to what is going to be developed next year. But what we do have is the capacity to hit a key stroke and say we will opt in or we will opt out. Right?

And what I am hearing from you is that your apprehension of the opt-in is it will diminish innovation. All right. And I am not quite sure why you say that. This is like a key stroke. The amount of information that they can get over the computer can include a key stroke from Peter Welch on opt-in or opt-out, right? It is not a big deal, really.

Mr. HANEY. Well, as we look at consumer behavior, when they are offered the opportunity to opt in, let's say one-third, for example, chooses to opt in. But when they are offered an opportunity to opt out, a very small percentage of consumers——

Mr. WELCH. No, exactly. You have precisely defined the issue. Who is going to be the default winner or loser on this? And if the technology company has access to the information and then can sell

it, then they are going to reap some reward for that. And you would like to think—or you suggest that that is necessarily going to be a better product for me? I am not sure that is right. But I would like to be the one making the choice.

So I think the number one issue is who bears the burden here, because I know the companies would prefer to get and use all the information they can.

And then number two is a basic question about rulemaking. There has got to be some flexibility. And there are a lot of folks here who don't believe that Congress or anybody else should be doing any rules any time, any place, for any reason. I am not one of them, all right. Because that means that it is kind of anarchy out there.

So do you have any opposition, you or Mr. McDowell, to some rulemaking authority as part of enforcement?

Mr. MCDOWELL. To the FTC?

Mr. WELCH. Well, we can have a debate about FTC, FCC, the uniformity. I am sympathetic to having a uniform standard, but there has got to be real enforcement, in my view.

Mr. MCDOWELL. Sure. So, historically, FTC has been the expert agency for privacy.

Mr. WELCH. Right.

Mr. MCDOWELL. So the FCC has had a very narrow aspect of this; only the common carriers and only regarding certain information for certain purposes under what we call CPNI. The whole rest of the universe in the privacy universe has been the FTC.

So I am not opposed to having the FTC with some limited rulemaking authority in this space.

Mr. WELCH. OK. I yield back.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Shimkus, you are recognized.

Mr. SHIMKUS. Yes.

Thank you, Madam Chairman.

To my colleague from Vermont, I wouldn't be so dismissive of the blockchain debate in this because—and, Peter, if you got a second, I am sorry to interrupt—because, the country of Estonia has full data protection on personal health records, on data; they are totally wireless, phone app, every government entity. And they are a small country, but it is all blockchain-developed. And if you are following cryptocurrency and that debate, that is all blockchain too.

So I do agree that we ought to be looking at this as far as this privacy debate somewhere in the future on a different data because this could solve a lot of the problems of—I am not the big cryptocurrency guy, but as far as an individual accessing other internet-provided government functions, I think Estonia has proven the safety of the use of this type of system. So I just want to throw that out since you mentioned it.

But I do want to go to Commissioner McDowell because of your former position in the FCC. So we have some questions.

You have heard that this committee held a hearing with Facebook a few months ago. And if you didn't hear, you should have heard. There have been reports that Facebook had collected call records and SMS data from Android devices and had the Facebook app installed going back for years. Our subcommittee

chairs just sent letters to Google and Apple regarding their collection handling of location data amongst other information that is at the core of their operating systems.

Given your experience as an FCC Commissioner, I expect you are pretty familiar with filings. My understanding is—and we are not, Members, we don't really follow how these filings occur. My understanding is that wireless carriers have a whole regime associated with serving these same devices. Those records are considered extremely sensitive personal information. They are CPNI and are subject to privacy regulations strictly enforced by the FCC.

What kind of reports are these entities required to file?

Mr. MCDOWELL. So, under CPNI—I am going to whip out my cheat sheet here because the Code of Federal Regulations can get kind of weedy. So they have to file an annual report. And, actually, under the FCC's privacy order from 2016, these reports were going to go away, and now they are back but only on common carriers. So that is just important, again, part of the asymmetry problem. But they have to first have an affirmation that the company, the carrier, has operating procedures in place to ensure that it is complying with the CPNI rules. Second, it has to explain how those operating procedures ensure compliance. Third, they have to report on any actions taken against data breach—data brokers, rather. And data breaches are another story. And, number four, report on customer complaints concerning data breaches.

And then, when it comes to data breaches, they have to first notify law enforcement and then wait 7 days before notifying the consumer. So there is a lot going on. But those are annual reports filed with the FCC.

Mr. SHIMKUS. What kind of consent must the provider obtain?

Mr. MCDOWELL. So, for instance, if you want to pay your phone bill through your bank online bill pay and you want to see your call detail, you can't do it through your bank website unless you go to your carrier, your phone company, your wireless company, whoever it might be, and give them consent to share that information with your bank, for instance. So that is a form of opt-in.

Mr. SHIMKUS. And you mentioned that, in case of breach, there is—they need to file notification of that, correct?

Mr. MCDOWELL. Data breaches, they do. Absolutely.

Mr. SHIMKUS. That is all I have, Madam Chairman.

And I yield back my time.

Mrs. BLACKBURN. The gentleman yields back.

Let's see.

Mrs. Dingell, you are recognized for 5 minutes.

Mrs. DINGELL. Thank you, Madam Chair.

I think that you have seen from this hearing that consumers are—and what we are talking about every day when we are talking to people that consumers are consistently losing control of their private information across the board. First, it was Equifax; then Facebook. Now we have talked about LocationSmart today, a third-party aggregator of cell site location information, which has made Americans' location data available to anyone with an internet connection. And I think that is what people don't understand. And when we are talking about where someone's phone is what we are really talking about is real location time any minute because I bet

most of us in this room have a cell phone in their purse or their pocket right now.

These breaches of trust cannot become normal. And I worry that, with each passing scandal, we are becoming numb to this gross invasion of privacy. I talk to people, and they say there is nothing we can do about it. But there is something that we can do about it. It is why we need to be talking, and I think too many people don't understand how much data there is and what people are doing about it.

So, Ms. Moy, I know you have answered questions, but I would like to dig in a little more.

Can you talk more about LocationSmart, how they obtain their information, and talk a little more about who had access formally but who informally or illegally could have gotten access to that information and what they might have done with it?

Ms. MOY. Sure. Yes. So, again, LocationSmart was providing access to information, location information, for virtually any mobile phone user in the country. So it had direct access to the location information provided by all of the major wireless carriers. And it was providing that information informally.

And this really seems like the carriers essentially outsourcing access to their customer sensitive information and the whole consent process, right? So, if the carriers don't want to deal with trying to get consent on a case-by-case basis, for example, applications that want to access the information from the carrier side or websites, that the carrier was outsourcing this function to a data broker, the LocationSmart company. And LocationSmart presumably is supposed to have been getting and keeping records of customer consent for every instance in which it was providing that location information. It was not doing so. LocationSmart was not doing that for a long period of time. We don't know exactly how long, but we do know that the securest platform that, again, would have enabled anyone—this is the sort of formal access to location information that you are talking about—would have enabled anyone who worked in a prison and had access to the securest location-based services platform to just type in a phone number and upload any documents—no one at the company was looking at those documents, according to the information that they told Senator Wyden's staff—and then get real-time location information for anyone.

So this was going on for a long period of time. Apparently, either the carriers didn't know about it or didn't care. The FCC either didn't know about it or didn't care. And with respect to informal access, the LocationSmart platform also was not secure. So some security researchers demonstrated that they were able to gain access to location information through the LocationSmart portal without having formal access to that system.

Mrs. DINGELL. Ms. Moy, let's keep building on that.

Do you believe cell site location information is covered customer proprietary network information under the statute?

Ms. MOY. Yes. I am really glad that you asked that question because it certainly is information about one's use of the telecommunication service that is accessible to the carrier only by virtue of the carrier-customer relationship. And it is information pertaining to the location of the user. So, under the statute, this does,

in my belief, meet the definition of CPNI. And so, to me, it does appear to be a CPNI violation that was happening on a massive scale.

Mrs. DINGELL. So do you believe there were violations of section 222?

Ms. MOY. It does appear that way to me.

Mrs. DINGELL. I will yield back my 29 seconds, Madam Chair.

Mrs. BLACKBURN. The gentlelady yields back.

Mr. Latta.

Mr. LATTA. Thank you, Madam Chair.

And thank you all for being with us today.

Mr. McDowell, if I could start my questioning. There are many ongoing conversations in the realm of data privacy. The Digital Commerce and Consumer Protection Subcommittee, which I chair, has held several hearings on these issues, and we will hear from the entire FTC next week about their work in the area.

In your testimony, you mentioned the formidable protections of the FTC. And I have been clear about my support for the FTC's enforcement authority and even introduced a bill to make sure that the FTC's jurisdiction remained in place in the face of the legal challenge.

Do you believe that the FTC is equipped to handle privacy matters for the vast portion of the economy under its jurisdiction from Main Street stores to some of the largest companies in the world, including common carriers, for their ever-increasing noncommon carrier activities?

Mr. MCDOWELL. So I think in terms of privacy, it is the expert agency on privacy, and it is very well equipped in a lot of ways. They have brought hundreds of actions against a variety of companies, including broadband internet service providers in the privacy realm and have fined them, et cetera. So, from that perspective, yes.

Again, going back to kind of the premise of my opening remarks, though, we do need some harmonization and modernization, I think, of standards. They are an agency roughly the same size as the Federal Communications Commission in terms of budget, in terms of number of attorneys and economists and engineers, although fewer engineers there than at the FCC. So they might need help in that regard as these issues become more thorny and more widespread.

Mr. LATTA. Thank you.

Let me follow up again, Mr. McDowell. I understand that under the current CPNI rules, telecommunication providers file annual compliance certifications. I also have a bill that strives to reduce the regulatory burdens on small businesses out there.

Do the rural telecom providers in my district have more stringent requirements than an edge provider offering similar services?

Mr. MCDOWELL. Yes. So that goes back to that dichotomy, that duality between what a telecom carrier has in terms of their obligations under section 222 versus an app provider that might be providing the same functionality, let's say voice, through an app that is not regulated by 222.

Mr. LATTA. OK. Not picking on you. Another question.

In your testimony, you discussed how you voted to extend the CPNI rules in 2007 when you were Commissioner to cover a practice where data brokers, otherwise known as pre-texters, were obtaining unauthorized access to CPNI and then turning around and selling personal telephone records.

In 2013, the FCC also found that the CPNI rules applied to data collected on a mobile device if directed by the carrier. Under the section 222 authority given to the FCC, how far can the FCC extend the CPNI rules to cover current and future practices and services impacting telecommunication services?

Mr. MCDOWELL. Excellent question.

So the Federal Communications Commission—it gets to be alphabet soup pretty quickly—is limited to applying section 222 to common carriers. If you are not classified as a common carrier, 222 can't apply. FCC does not have the authority. Only Congress could change that if it wanted it to.

Mr. LATTA. OK.

And, Madam Chairman, I yield back the balance of my time.

Mrs. BLACKBURN. The gentleman yields back.

Ms. Eshoo, you are recognized.

Ms. ESHOO. Thank you, Madam Chairwoman.

And thank you again to the witnesses and to Commissioner McDowell. It is really a special pleasure to see you again and to have your daughter with us as well.

I am so frustrated listening. I have learned. But the whole case of privacy and what the Congress has done, I really think, needs to be restated. Congress is responsible for having wiped out privacy protections for the American people, period. That is why we are where we are. The CRA wiped it out. Whatever was left or whatever net neutrality contained in it relative to any protections, scorched earth, gone.

Now we have the BROWSER Act. It does nothing meaningful for real privacy. There is no rulemaking authority. There is no civil penalty for enforcement. There is no data security. It preempts any kind of state laws. California just passed something which is very strong. And, actually, when the strong bill came out, the interests went to work to water it down to a few drips of water, and Californians were outraged. And there was such pressure on the state legislature based on what Californians said that it came out strong. But the BROWSER Act preempts that. It also preempts the FCC, the expert telecom agency.

So where are we? Seventeen months and counting, blah, blah, blah, blah. Anyone that has voted, in my view, for these things has to answer to their constituents when they complain to us, Independents, Republicans, conservative, right wing, left wing, Democrats, everyone, when they say: This is what has happened to me.

So, let's be honest about where we are. All right. So everything has been wiped out, in my view. There isn't anything protecting anyone. Where do we go from here? I don't think 220(b), whatever it is—that really covers something very small. We are talking about a landscape that is very different, as you said, Commissioner McDowell, when that was placed on the books.

I don't believe that there is a reason that some people want the FTC. The FTC doesn't have what it needs to enforce a darn thing,

in my view. And I don't know if Congress is going to step up and give them all these authorities that the FCC had.

All of a sudden, they love the FTC. FTC can't do a damn thing. It doesn't have any teeth to do it. They have asked Congress for a false set of teeth, but they haven't been purchased yet.

So, Ms. Moy, where do you go from here? Where would you start building something?

Ms. MOY. Thank you for the question. Thank you very much.

Ms. ESHOO. Yes. Well, I am so darn frustrated. And it is like we are dancing around something that is really lovely, and we are just going to plant a few flowers, and then everything's going to bloom. Everything's been wiped out. That is why we are in the place that we are.

Ms. MOY. I think you are right. So the internet does raise a bunch of important questions about privacy. But just because we now have apps that collect health-related information and wearable health devices, we don't have doctors in here complaining that they should not be subject to HIPAA. And we do not have schools in here asking that they not be subject to not be FERPA, the Federal privacy law, just because there are now educational apps and educational data is being collected over the internet.

We shouldn't do away with the existing privacy regulations that we have just because we are lacking privacy across the board. We need to keep and build on the privacy protections that we do have. And that is where I would say that whatever we are going to have moving forward, it has to have rulemaking authority, strong enforcement authority, as you say, including civil penalties. And it ought to have a role for the state attorneys general who have much greater resources across the 50 states and territories than one Federal agency can have alone.

Ms. ESHOO. Let me just give Commissioner McDowell a few seconds. I know that we may not agree on some of this, but I want to hear what you have to say very quickly.

Mr. MCDOWELL. So the CRA overturned the requirements on carriers only. This wasn't the entire internet ecosphere. So that goes back to the FTC.

Ms. ESHOO. So what is left? What is left? Who is protected and how?

Mr. MCDOWELL. So through the Federal Trade Commission. So that is broadband and all the rest. So that is through the Federal—if you think the FTC needs more resources or a different statutory standard, then that is certainly Congress' prerogative.

Ms. ESHOO. OK.

Thank you very much.

Mrs. BLACKBURN. The gentlelady yields back.

Mr. Guthrie, you are recognized.

Mr. GUTHRIE. Thank you, Madam Chairwoman. I appreciate that.

And, Commissioner McDowell, in your testimony, you mentioned Marty Cooper and the first cell phone. You also discussed how competition is an important part of how CPNI rules came into existence. In addition to protecting consumers' privacy, the rules were originally intended to promote competition in the emerging enhanced services market by preventing the regulated side of AT&T

from sharing information with its nonregulated information services side.

And we have come a long way since the device Mr. Cooper had. But a legal landscape that reflects this evolution is not necessarily followed. It appears edge providers are freer to innovate as information is shared across all sorts of affiliated entities.

What effect does the current regulatory structure have on thwarting new entrants?

Mr. MCDOWELL. So if the new entrant is not a common carrier, section 222 does not apply. So we have lower regulatory barriers. You are probably going to see more innovation and investment. That has sort of been the story of the internet ecosphere, or other markets as well. You could make a lot of case studies there.

So, if there is a new entrant in the telecom market, they would have to live under section 222.

Mr. GUTHRIE. So it is a disadvantage versus the edge providers for——

Mr. MCDOWELL. It is a different—yes. It is a slight——

Mr. GUTHRIE. The more restrictive——

Mr. MCDOWELL. Yes. It is trickier.

Mr. GUTHRIE. More restrictive regulated.

If you argue unregulated allows you to—or lower regulation allows more entrants, then they are more regulated.

Mr. MCDOWELL. Correct.

Mr. GUTHRIE. OK. So, Mr. Haney, what is the functional difference between placing a call from a smartphone using my wireless carrier's network and using a third-party app?

Mr. HANEY. The only difference is legal. And using the carrier is subject to the full panoply of FCC privacy regulation; using an app that is not interconnected to the public switch telephone network is subject to the FTC the same as the rest of the internet ecosystem.

Mr. GUTHRIE. So completely similar products are completed——

Mr. HANEY. Completely different treatment.

Mr. GUTHRIE. Different treatment.

Should my information be subject to different privacy protections depending on the network that I use?

Mr. HANEY. No, sir, I don't believe so.

Mr. MCDOWELL. If I could put a finer point on it, though. If it is unlicensed—so you can have that transmission, as I tried to point out earlier through unlicensed. You are not a subscriber. That is not common carriage. It is not regulated. But the same functionality to the consumer, that would be unregulated.

But if it is through a carrier, it doesn't matter how that carrier is supplying it or providing a service, then then section 222 would apply.

Mr. GUTHRIE. It is treated differently.

I guess my point I am trying to get at is the same product is treated differently based on——

Mr. MCDOWELL. How it is done.

Mr. GUTHRIE. So, also, Mr. Haney, you stated the goal should be to prevent regulations from hamstringing some market participants but not others. And the logical way to do that is by ensuring that all participants in the internet ecosystem are treated the same.

Is there a role for Congress to achieve that goal through legislation, or is that preferable to rely on the Commission?

Mr. HANEY. Sir, the FCC cannot do it. The FCC does not have legal authority to enhance privacy more broadly speaking than just telecommunications common carriers. So, if the goal is to provide the FTC with rulemaking authority, civil penalties, what have you, then that would require an act of Congress.

Mr. GUTHRIE. OK. Thank you.

Well, I appreciate your answers to my questions.

And I concluded my questions, and I yield back.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Butterfield, you are recognized.

Mr. BUTTERFIELD. Thank you very much, Madam Chairman.

And thank you to the witnesses for your testimony today.

As consumers, we are inundated with privacy policies from the companies with which we do business, whether it is financial institutions or doctors or hospitals or even ISPs and edge providers. We are forced to read these long legal documents on small mobile device screens. And the older you are, the worse it is. Trust me, I know.

Sometimes we are even told that we cannot access a certain essential application for work or otherwise without quickly agreeing to the question. So I don't have it directed to either of you. If anyone wants to respond, you certainly can. Do you think consumer privacy disclosures are effective in letting consumers know the kinds of information about them that is collected, how it is used, and whether and with whom it is shared?

Ms. MOY. I think you are raising a really good point about the deception standard, right, which is the FTC, the Federal Trade Commission, just has this authority to prohibit unfair and deceptive trade practices. So, when it comes to privacy, most of the time for consumers what that means is that our privacy is only protected insofar as we are reading privacy policies, agree with what is in them, actually have a choice about whether or not to agree to that—in theory, we have a choice—and then that the company doesn't do something with our information other than what they claim.

And so this is why it is so important. We all know that there are so many instances in which we share our information, but we really don't have a choice. We don't have the time to read those privacy policies. Maybe we can't read them. They are very difficult to read. Maybe we are required, as you say, to have access to a service for work. And when we really do have no choice but to share information with a business that is going to use it for some other purpose, then it is so important to have standards in place that prevent that information from being used in other ways without our permission.

Mr. BUTTERFIELD. What say the Hudson Institute? Do you have some thoughts?

Mr. MCDOWELL. So one aspect of all this debate, by the way, too, is the aspect of contract law and tort law. So every day there are class action lawsuits filed against a variety of market players in this space or other spaces too.

So the idea of foreign contracts in any industry, whether it is the internet or something else, anything, that is as old as America, if not older.

But, also, the idea of class actions as well as being a deterrent against these wholesale violations of contract or of common law that a contract might fly in the face of common law. So this is a whole other aspect of this whole debate which is important to know.

Mr. BUTTERFIELD. OK.

Mr. HANEY. May I just add that there may very well be a need to create more baseline regulation to satisfy what we can all agree consumers expect to remain private. But there is no way the prospective regulation can anticipate everything that is going to happen in the marketplace. So there is, I think, an important role for user agreements.

And, also, in addition to class action lawsuits, press reaction, consumer outrage, the kind of response we have seen to secure it, all of those things I think play a role in terms of protecting privacy.

But I agree with you. I don't read the user agreements. They are incomprehensible most of the time.

Mr. BUTTERFIELD. That kind of leads me into my second and last question, and that is, are you aware of any, I am going to say serious research, or do you have any ideas of how to make privacy policies more consumer friendly?

I know there is a lot of chatter about it, a lot of conversation. But is there any serious research going on about how we can go to the next level?

Yes.

Ms. MOY. I know that there has been some good research here, including by a team of computer scientists led by Lorrie Faith Cranor at Carnegie Mellon on privacy policies. But I am not sure that there are any great solutions right now. Unfortunately, the legal complexities associated with these disclosures are extremely difficult to translate into a user-friendly——

Mr. BUTTERFIELD. That is what I needed to hear.

Any agreement with what she just said?

Mr. MCDOWELL. It is complicated, to paraphrase Avril Lavigne.

Mr. BUTTERFIELD. It is complicated. OK.

Do you associate yourself with Mr. McDowell?

Mr. HANEY. Yes, sir.

Mr. BUTTERFIELD. Thank you.

I yield back, Madam Chair.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Johnson, you are recognized.

Mr. JOHNSON. Thank you, Madam Chair.

Hopefully, I can see around to see all of you, but thanks for being here with us today. Important topic that we are talking about.

Section 222 defines CPNI in part as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunication service subscribed to by any customer of a telecommunication's carrier and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."

Mr. McDowell, is this information similar to the information obtained by app developers and other edge providers who know, by nature of their relationship with the users of their platform, just how much consumers are using the app, when they are using it, where they are using it, and what they might even be searching for on that platform?

Mr. MCDOWELL. It can be similar. And app providers and websites can actually gather even more data. And the reason being, it is increasingly true because more and more Web traffic is becoming secured, in other words, to where an ISP can't see what is transversing across its networks.

So what app developers can gather is a larger umbrella than what is covered by CPNI, which is viewed as a smaller subset of data, but very important data.

Mr. JOHNSON. So should we have similar rules to protect that kind of data? They seem awfully similar.

Mr. MCDOWELL. So you are asking if we need CPNI rules to apply broadly to everybody. Is that what you are asking or the other way around?

Mr. JOHNSON. Well, should it apply to this kind of data that I just described to you——

Mr. MCDOWELL. Yes.

Mr. JOHNSON [continuing]. Third-party edge provides are collecting?

Mr. MCDOWELL. Yes. I think you need clarity here so that everyone knows what the rules of the road are.

Mr. JOHNSON. OK. All right.

And again to you, Mr. McDowell. Do consumers differentiate between the various voice and texting services available on their phones, or do they view, for instance, Verizon mobile service and Google Voice as essentially the same service?

Mr. MCDOWELL. The same functionality from the consumer's perspective.

Mr. JOHNSON. OK. Section 222 protects the private information contained in traditional subscriber line bills. It also protects the location information of customers. Today's smartphones provide a host precise geolocation information on each device. This precise geolocation can locate a person within feet of their actual location. The network providers cannot access this information, yet we know the Android operating system does in order to serve ads to the device.

Is there a reason why the operating system should have this sort of precise information but not the carrier?

Mr. MCDOWELL. So it is an excellent question. Your device can triangulate off of WiFi signals, cell towers, Bluetooth, any sort of radio frequency energy that is emanating if it knows where that is coming from. Then it can triangulate and tell you where this device is right now.

So carriers can tell where you are vis-ă-vis a cell tower but not necessarily specifically where you are. This has a lot of implications with 9-1-1 location accuracy and things like that. So there are times when you want everyone to where you are, and there are times where you don't want anyone to know where you are. And it shouldn't matter if it is telecom carrier or an app provider.

Mr. JOHNSON. Today, I don't know that consumers know who knows where they are. I am not sure they know where they are in this kind of interconnected environment.

Final question: What do you think of the consumer being given opt-in rights for this data in order to choose for themselves who they share it with?

Mr. MCDOWELL. And we talked about this earlier, and the finer point on the discussion from earlier, which is opt-in gives consumers a lot of power for each time this issue comes up, right? So that is a good thing.

The downside to it—and this is where we as policymakers, folks have to wrestle with it—is the idea of opt-in fatigue. If you think of how many usernames and passwords you have for various websites and apps and everything else, and they change a lot—you should be changing them a lot if you are not—that is exhausting.

So opt-in can become exhausting. Can there be a mix, maybe a blend of opt-in or safe harbor, for instance, as well, that you know you are going to get a certain standard of protection in a safe harbor that does not require an opt-in? That is one idea which I think deserves some discussion.

Mr. JOHNSON. OK. All right.

Madam Chair, I yield back a whole 10 seconds.

Mrs. BLACKBURN. The gentleman yields back.

And, Mr. McNerney, you are recognized.

Mr. MCNERNEY. I thank the chair.

Ms. Moy, every day consumers are faced with another data breach undermining the choices they have about their privacy. But despite this troubling trend, last year, the Republicans in Congress voted to do away with reasonable data security requirements for internet service providers.

So how did the data security rules protect consumers before they were overturned?

Ms. MOY. Thank you.

Yes. So the broadband privacy rules would have required broadband providers and phone providers to take reasonable measures to protect their customers' information from unauthorized use, disclosure, or access. And they also would have required providers suffering a breach to notify affected consumers within 30 days. There were a bunch of factors to determine what reasonable security measures might look like in the rules, but, unfortunately, as you said, those rules have been eliminated.

Mr. MCNERNEY. Are the ISPs subject to any data security rules today?

Ms. MOY. No. There are no concrete rules right now that apply to broadband providers.

Mr. MCNERNEY. So it is the Wild West then, isn't it?

Ms. MOY. It is, in fact, the Wild West when it comes to data security.

Mr. MCNERNEY. OK. Can you explain why it is wrongheaded for Congress to repeal privacy rules in the name of protecting consumers?

Ms. MOY. So, a colleague of mine had a great analogy here, which is, if you have a house with a broken roof, you don't raze the house to the ground; you fix the roof. And I think that we are look-

ing at something similar when it comes to privacy. Consumers are concerned about loss of control over their private information across the board. That suggests a need for greater and stronger privacy protections everywhere.

And as I said, I do think that it is important to modernize the Federal Trade Commission by giving it important tools, like rulemaking authority and strong enforcement, civil penalty authority. But we should not be doing away with existing privacy laws we have, like broadband privacy, but also health privacy, education privacy, and so on.

Mr. MCNERNEY. Well, there are some privacy proposals, such as the BROWSER Act, that don't include specific protections for data security.

Do you think consumers have meaningful privacy protections without data security protections?

Ms. MOY. No. You know, I think privacy and data security go hand in hand. What consumers are complaining about is a loss of control over their information. And that loss of control can come in the form of a business failing to get a customer's consent to use their information in a way that the customer didn't anticipate. But it can also come in the form of a business failing to safeguard the information from unauthorized access by malicious attackers or even by employees within the company as was the case with AT&T a few years ago in a case that ended up resulting in an FCC enforcement action.

Mr. MCNERNEY. What are some of the guiding principles that we should be considering whenever thinking about data security legislation? You have already given those, but——

Ms. MOY. I have. But one that we haven't talked a whole lot about, I think, is really preemption. Although this is not the topic of this hearing today, this subcommittee has considered a number of pieces of legislation to standardize data security and breach notification requirements that apply to companies.

But, unfortunately, many of those proposals would eliminate state law on data security and breach notification. And there are so many great and wonderful strong, innovative laws that are taking place at the state level that preempting all of those laws would be a net loss for consumers.

Mr. MCNERNEY. Well, you have a way of answering the question right before I ask.

You testified that the State AGs should have enforcement authority. Does the BROWSER Act do this?

Ms. MOY. No, unfortunately not.

Mr. MCNERNEY. Thank you.

Mr. McDowell, in addition to section 222 of the Communications Act, there are also important data security protections under sections 631 and 338. How important are these protections for consumers? And what can the FCC do to ensure that they are being followed?

Mr. MCDOWELL. They are similar in spirit. So 631, for instance, is regarding your video viewing habits, what you view. So it is about protecting consumer information. The FCC has enforcement authority, fining authority, et cetera, over those sections.

Mr. MCNERNEY. OK. Good. You think those are good and should continue to be enforced. But the FTC doesn't have the resources to enforce.

Mr. MCDOWELL. Well, look. The FCC and FTC are similarly sized and almost identically sized agencies. So, again, and also back to the state preemption issue. It is a matter of how many agencies you are going to have with different standards for different piece parts of a converging internet ecosphere, and that is what becomes confusing.

Mr. MCNERNEY. All right. I will yield back.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Long, you are recognized.

Mr. LONG. Thank you, Madam Chairman.

Mr. Haney, it is my understanding that the location information considered CPNI, if it is associated with a call over the telephone network. But it seems like tech companies have the ability to track location information not just associated with their app but with a variety of apps or an entire mobile device in some instances.

Who has better insight into location information, telecommunications providers or tech companies?

Mr. HANEY. Sir, I believe it is tech companies.

Mr. LONG. Under current law, what authority governs the collection of location information by smartphone manufacturers, operating systems, or apps?

Mr. HANEY. That was the Federal Trade Commission.

Mr. LONG. How does the authority differ from FCC's CPNI requirements?

Mr. HANEY. The FCC's CPNI requirements are prospective regulation. It is very clear. The FTC recognizes that this is a dynamic marketplace—the technology is always evolving—and that it is impossible to anticipate everything and draft a regulation to address it. And so the FTC tries to be more flexible and to respond after there is a problem instead of trying to anticipate every problem.

Mr. LONG. OK. Thank you.

Madam Chairwoman, I yield back.

Mrs. BLACKBURN. The gentleman yields back.

Ms. Clarke, you are recognized.

Ms. CLARKE. I thank you, Madam Chairwoman. And I thank our distinguished panelists for their testimony here today. Let me also thank our ranking member for convening this important hearing regarding privacy, an important topic for all Americans.

Under the FCC's broadband privacy protections, broadband providers had to get opt-in consent sharing most types of consumer's data. Unfortunately, our Republican colleagues in Congress wiped those privacy protections off the books.

Ms. Moy, when I am using my internet connection at home today, are there any clear opt-in or even opt-out requirements that apply to how my ISP collects and uses my data?

Ms. MOY. No. There are not.

Ms. CLARKE. OK. And what are the rules that apply to my broadband provider when it collects or uses my data? Specifically, what can the FTC require under section 5 of the FTC Act?

Ms. MOY. At this point in time, there are no rules. The FTC can prohibit unfair and deceptive trade practices. But it has very little

power to do anything where there are privacy violations unless a business has actually exceeded what it told consumers in its privacy policy, which, as we know, most people don't read.

Ms. CLARKE. Oh, boy.

Over the past several years, the extent to which corporate conglomerates will discriminate to improve their bottom line has come into focus. Whether it is broadband providers, redlining low-income communities, or Facebook discriminating against certain groups when it comes to housing advertisements, the result is marginalizing families in their communities.

I am concerned that the lack of meaningful privacy protections is only going to make these problems more pervasive. For that reason, I think Americans are in desperate need of strong privacy protections wherever they go online.

Ms. Moy, can you tell me how sacrificing privacy protections, like our Republican colleagues did with their privacy CRA, can have a desperate impact on some consumers, particularly those in communities of color?

Ms. MOY. Thank you, Representative. That is a really important question. And I think that it really helps us put a finer point on what we are really concerned about when we are thinking about harms associated with privacy violations.

When a business, whether it is a broadband provider or another type of company, has information about our private lives and they use that information to target content and advertisements to us, the targeting may result in reinforcing existing social disparities, right? Keeping us in our boxes. Limiting the educational opportunities that are available to us, the job training opportunities and, indeed, the job opportunities themselves, financial opportunities. And these are some of the results that may come from collecting information from consumers.

I think that that is why it is so important to have strong privacy rules where, as with some entities in the ecosystem, consumers really have no choice but to share information about their private lives that could reveal things like sensitive demographic information or financial status.

Ms. CLARKE. Thank you.

As we consider legislative solutions to protect privacy, I am guided by the belief that any successful solution must not require our constituents to become lawyers or engineers in order to understand their rights and to protect themselves and their personal information. The privacy rules of the road can change dramatically depending upon where someone goes on the internet. Rather, consistency, uniformity, and technological neutrality are keys to any privacy solution. Do you all agree on the panel?

Mr. HANEY. Yes.

Mr. MCDOWELL. Yes.

Ms. MOY. Yes.

Ms. CLARKE. Very well.

Madam Chair, with that, I yield back.

Mrs. BLACKBURN. The gentlelady yields back.

Mr. Costello, you are recognized.

Mr. COSTELLO. Thank you, Madam Chair.

Mr. McDowell, as Mr. Doyle referenced earlier, and, to me, what was just discussed about selling location data to third parties sounds more like an issue of consent and how we can make sure consumers truly understand what they are consenting to before they use a service. I think Ms. Moy alluded to that in terms of third-party consents. Oftentimes you don't even know what you are consenting to.

But I also understand that the FCC, and possibly even the FTC, are looking into what exactly occurred here. And will we have them both in front of the committee soon so we can ask additional questions of the investigation at the time? This is my question. I think this highlights the asymmetry in the current rules. If this was an edge provider who had shared location data, would it be subject to the same regulations?

Mr. MCDOWELL. Not section 222, no.

Mr. COSTELLO. Could you point to any regulation that it would?

Mr. MCDOWELL. Not unless it has some affiliation with a carrier, so no.

Mr. COSTELLO. OK. Related also to section 222. CPNI, VoIP, et cetera, when you break it down—my smartphone here. If I tap the phone app icon to make a call, there is one set of rules. But if I tap the Google Voice app icon to make the call, which I don't do, there is another set of rules.

Can you talk about the practicality of having separate regulatory regimes in that sense? And should consumers expect their data to be treated the same regardless of what technology they use, to use the term "technology neutral"?

Mr. MCDOWELL. Absolutely. Again, to your point, to the consumer, there is no difference. It is the same functionality. You want to convey a voice message in real time, have a conversation with somebody in real time. So it doesn't matter whose app or whose network or if it is licensed or unlicensed or it is through a carrier or through an edge provider—by the way, I think they are all tech companies. I know we try to draw distinctions between ISPs and the tech community. I think they are all technology companies. And they are all great American success stories. But nonetheless, from the consumer's perspective, there shouldn't be any difference regarding what information——

Mr. COSTELLO. And so the regulatory framework should be uniform.

Mr. MCDOWELL. I agree, yes.

Mr. COSTELLO. Up and down.

Mr. MCDOWELL. Yes.

Mr. COSTELLO. Ms. Moy alluded to, in her statement, the issue—and we have read it elsewhere—with states attorneys general. And, Ms. Moy, I will give you the opportunity to address this as well.

I understand that taking FTC regulations and having someone else enforce it at the FTC, the argument goes, isn't being aggressive enough? But do you have concerns with that? And then, after you answer that, Ms. Moy, aren't there some differences, though, with the statute that you are referencing just in terms of the technical expertise required to interpret vis-ă-vis the statute that you were pointing to.

So Mr. McDowell and then Ms. Moy.

Mr. MCDOWELL. Sure. And state attorneys general can do a terrific job protecting consumers on a number of fronts. My concern, though, is having 50 different standards or——

Mr. COSTELLO. Totally.

Mr. MCDOWELL [continuing]. More with all the territories. And that is going to really harm American global competitiveness in this space. So, again, back to uniform standards, not 50-plus standards state by state in the internet, which is borderless, right? It is an interconnected network of networks. The packets fly all across——

Mr. COSTELLO. Isn't there also a fair amount of interpretational flexibility with those 50 attorney generals? The statute that Ms. Moy is referencing is pretty straightforward, as I understand it.

Mr. MCDOWELL. I think to your point, if you are saying if there is going to be one standard, a national standard, but state attorneys general could enforce it, that is another conversation altogether.

Mr. COSTELLO. Ms. Moy, your comments.

Ms. MOY. Thank you.

So, I think that part of the issue here is that the FTC, while it does a lot of great work on privacy, it has a staff of just over 1,000, if I recall correctly. It doesn't have an office of engineering and technology. It doesn't have an engineering department at all. And its jurisdiction ranges as broadly—although it does a lot of internet privacy work, it also polices, for example, the consumer-facing statements made about pomegranate juice, right? It has an incredibly broad jurisdiction with very limited tools to enforce.

So it is really important to have additional enforcement actors, additional cops on the beat, as it were, to ensure that businesses subject to the regulations passed by the commission are, in fact, being followed.

Mr. COSTELLO. But wouldn't you think if the FTC needed those additional policemen, as you used the term, they would request them, or they would find a way in their budget to have them?

Ms. MOY. So, yes, perhaps.

Mr. COSTELLO. Might that be called something different than—you referenced the FCC division there. Might they be operating in a different division with the same type or better expertise on enforcement?

Ms. MOY. Perhaps. But another thing that state attorneys general do is they talk to businesses that are based in their state. They do a lot of guidance in addition to enforcement.

Mr. COSTELLO. Thank you. I yield back.

Mrs. BLACKBURN. The gentleman yields back.

Ms. Matsui.

Ms. MATSUI. Thank you, Madam Chair. And thank you to the panel for being here today.

We have talked about many things, and maybe I might be repeating myself. But I think we should listen and try to figure out from you all where we might be going forward because when you look at it, this concept of protecting proprietary consumer information began with the monolithic telephone era, which was pretty far back. And with the 1996 Telecom Act came a more precise focus on CPNI protections against unauthorized use, access, and disclo-

sure. And it includes, among other types, phone numbers, dial and duration of calls placed to these numbers.

But we all know that most consumers don't make any distinction at all between where these phone calls are delivered in packets, over the internet, or through switch access lines.

But we all understand the need for context-specific privacy regulations that are responsive to the types of consumer relationship and sensitivity of information collected and shared to actually afford consumers the privacy protections they expect and they figure they are getting, for some reason.

Ms. Moy, as different technologies provide similar services, what distinctions remain necessary or become unnecessary to protect sensitive consumer information?

Ms. MOY. That is a very good question. And it is a really hard one that we are all grappling with right now.

But, nevertheless, I do think that consumers have different relationships between the carriers that they contract with, that they pay a monthly subscriber fee to, that they expect they are paying for service as they do with the entities that are doing business over the internet. Just as when you send a letter in the mail to a friend, you have different expectations about what the mail carrier will do with the address information and the date on the outside of the envelop. So does the consumer have different expectations about what, again, the entity that they are just paying to transfer the data on their behalf will do with their private information as opposed to the companies with which they do business.

That said, I do agree that there are certain services that consumers use now that have become so pervasive, so dominant that they are essentially unavoidable. And I look at unavoidability as, really, one of the key factors when it comes to considering what level of privacy protections should apply. When services truly are unavoidable for consumers and they have to share sensitive information, then I think that heightened privacy is appropriate, just as with healthcare, education, and finance.

Ms. MATSUI. OK. Could you get into more detail there? What do you think is unavoidable here that we are talking about?

Ms. MOY. So, without talking about specific entities, I do think that there are certainly certain advertising platforms that are so pervasive as to be essentially unavoidable for consumers to share information with. It was Congressman Butterfield referenced certain services that consumers feel they must take part in because an employer requires it, for example. That may rise to a level of unavoidability for a consumer. And I think that, when we start seeing services rise to the level of being essential or unavoidable, then we require heightened privacy.

Ms. MATSUI. OK. Mr. McDowell, Mr. Haney, any comments on this?

Mr. MCDOWELL. So I am not sure if this is what was said, but I want to make sure we understand that there doesn't have to be a difference between who you pay money to for a service versus you are giving your personal data for a free service. You are actually surrendering something for free services as well. So they are not entirely free.

But, again, back to one uniform consistent tech-neutral standard, I think that is the way to go.

Mr. HANEY. I agree.

Ms. MATSUI. OK. CPNI rules enacted require opt-in consent from consumers before a carrier can share information. But we know that it is often the case the third party to an online platform can and does receive data and information on the consumer. And the website may be used as an analytic tool from a third party; the website servers could send information on the user's visit back to the third party and allows that third party to access data similar to that gathered by the website.

While this may be commonplace, it means that each user may have information aggregated by a party with whom they have no direct relationship or knowledge. There are a lot of parties here. So the third party accesses consumer data with whom the consumer does not have a direct relationship. How do consumers have a meaningful choice in how that data is used?

Ms. MOY. That is a great question. That really gets to the heart of what the problem is with falling back on a general deception standard without rulemaking authority or anything else for the FTC to clarify—clarification, perhaps of its unfairness authority, rulemaking authority for it to create rules around things like data brokers and data security as well would be necessary.

Ms. MATSUI. OK. Thank you.

It looks like I have run out of time. Thank you very much.

I yield back.

Mrs. BLACKBURN. Mr. Flores, you are recognized, 5 minutes.

Mr. FLORES. Thank you, Madam Chairman. I want to thank the panel for joining us today.

When I do something with this phone, there is—I see four groups of people that is harvesting data from it. So not only is the cellular carrier getting information, but your app provider is getting information. The iOS folks, the operating system folks, are getting information, and theoretically, the ISP is as well if it is connected to Wi-Fi.

So you have all talked about the need for a technology-neutral solution to address privacy. So I would like to get into the weeds a little bit today.

As a policymaker, what are the three or four most important things that that policy should have to protect the privacy of the American consumer?

So we will start with you, Ms. Moy. And let's go quickly, because I have some——

Ms. MOY. At the risk of sounding like a broken record, I think it is crucially important to, first of all, I do think that sectoral laws have a place and are really important to protect consumers in instances like health, education, finance, and telecommunications where there are heightened privacy obligations and requirements.

But in addition, I think that whatever baseline we are going to have, if it is to be administered by an expert agency such as the Federal Trade Commission must include rulemaking authority to provide flexibility, regulatory agility, as we think of it, as well as robust enforcement tools, including civils penalties.

Mr. FLORES. OK. Mr. McDowell.

Mr. MCDOWELL. Sure. Transparency, uniformity. But also, most importantly, probably consumer choice. I would support rulemaking authority for the Federal Trade Commission but in a very limited way.

Mr. FLORES. OK. All right.

Mr. Haney.

Mr. HANEY. Yes, sir. I think that enforcers should consider burdens on industry as they affect consumers, as they may affect innovation. I think that the FTC has got it right in looking at the sensitivity of the information at issue, so I think that is very important.

Secondly, I think it is very important that the rules apply equally to every participant in the market so that everybody has the same opportunities to innovate and to earn a fair return on investment.

Mr. FLORES. OK. Great.

Mr. McDowell, we had a question a few minutes ago about 50 states attorneys general being used to pursue policy relief for consumers. California has passed a law 2 weeks ago.

Would you agree that that is the wrong approach as well, to have 50 different state standards?

Mr. MCDOWELL. Yes, I disagree with that approach.

Mr. FLORES. OK. You were going down a direction a few minutes ago talking about blockchain, and you got cut off, unfortunately. And it seems to me like blockchain may be one of the technology solutions that addresses a lot of these policy issues.

Can you expand on that? You didn't get a chance to before.

Mr. MCDOWELL. Sure. Real quick.

So, first of all, it is already part of our lives. And as we start to roll out the Internet of Things, you are going to see more and more blockchain applications. And there is a tremendous amount of entrepreneurism and investment in this space, a lot of experimentation. And it is actually very pro-consumer, empowers consumers tremendously. And it is different from encryption. Technically, they are two different things. So I think it will solve a lot of issues.

And the quick backdrop on that is I think the first time I testified before this committee was 1998, so 20 years ago this summer. I am just recalling, in front of Chairman Dingell. And it was on slamming, which was the unauthorized switching of your long-distance carriers. That is not as much of an issue any more, right? So long distance isn't even a thing anymore. So markets change. Technology changes. So I think blockchain is going to be tremendously helpful as it develops.

Mr. FLORES. OK. Is there any change in your answer regarding what we should have in a 21st century privacy policy solution in light of the fact that blockchain is on the horizon?

Mr. MCDOWELL. Well, flexibility and light touch. And I tried to put that in my pre-filed remarks, that light touch, we have to make sure we are not cutting off innovation and experimentation and investment.

Mr. FLORES. Exactly.

Ms. Moy, a question for you. In the context of the FCC's broadband privacy proceeding, you argued against pay for privacy because of a lack of broadband service options.

What are your thoughts on a pay-for-privacy solution when it comes to Facebook and other similar providers?

Ms. MOY. Thank you for that question. I think that that is a really good one.

My concerns about pay for privacy—so I do not believe that privacy should be a luxury available only to those individuals who can afford it. That is the place where I start with when I am thinking about pay-for-privacy issues. That is particularly the case where, as with broadband, you are looking at an essential service. So—and something where consumers really can't avoid sharing information about themselves. If consumers have no choice but to share information with a broadband provider in order to participate in the modern economy, then they should not be required to pay a premium that they cannot afford in order to protect that information from additional uses.

And so my position on pay for privacy in the broadband context was that premiums that may be charged or discounts given should not be coercive in nature to consumers nor should they make privacy options essentially practically, as a practical matter, unavailable to consumers who cannot afford them.

I think that if we are looking at other services, then the threshold question is, is this service essential, a service that consumers cannot avoid sharing information with? If so, then I would have the same feelings about pay for privacy.

Mr. FLORES. Thank you.

I think with regard to competition in the broadband space, as 5G rolls out on the near-term horizon that we are suddenly going to see that extra competition that will help the—absent a solution on privacy for the ISPs, I think we are going to have a market solution that helps us get there.

That is the last of my questions. I yield back.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Engel.

Mr. ENGEL. Thank you, Madam Chair.

Companies across the globe are changing the way they collect and use consumer data, and we are seeing more sophisticated practices, which obviously results in more challenges to American's privacy.

Ms. Moy, you testified that agencies tasked with protecting consumers' private information should be given rulemaking authority. And you referenced remarks from Commissioner Maureen Ohlhausen when she asked Congress to give rulemaking authority to the FTC.

So my first question to you is whether you think that rulemaking authority should be given to the FTC, the FCC, or both.

Ms. MOY. So I think that each agency needs rulemaking authority for the areas in which it has expertise. We have separate expert agencies for reasons. The Federal Communications Commission has greater network expertise and communications expertise. And, again, has this Office of Engineering and Technology, a whole staff of network engineers that the Federal Trade Commission lacks.

The Federal Trade Commission, on the other hand, is responsible for enforcing this baseline general privacy standard across the en-

tire ecosystem, including, as I was saying before, the marketing of products like pomegranate juice.

So the Federal Trade Commission needs rulemaking authority for general things, like data security obligations that ought to apply to all entities. It probably needs a clarification of its unfairness authority, particularly in light of recent court decisions that call into question how strong its authority is under that, under the statute.

The Federal Communications Commission still requires rulemaking authority to implement those sections of the Communications Act that it is responsible for implementation and enforcing.

Mr. ENGEL. Does the FTC have the resources it needs for enforcement? For instance, I was told that the tech lab only has six people in it.

Ms. MOY. That is right. That is right.

I think the Federal Trade Commission is doing the best job that it can with a relatively small staff, but, again, a staff of 1,100 people for the entire agency can't possibly be enough to police all of the unfairness and deceptive potential practices of all companies across the entire country, including privacy of the entire internet ecosystem.

Mr. ENGEL. Ms. Moy, let me continue.

As you know, one of the proposals that we are considering in this committee is the BROWSER Act. And if you can, could you discuss the rulemaking authority contained in the BROWSER Act and whether it will make for better and clearer privacy enforcement?

Ms. MOY. Right. If I am correct, the BROWSER Act does not give rulemaking authority. I think that that is problematic. I think that any—as I was saying before, I think that any privacy law that we have in this area ought to have rulemaking authority and civil penalty authority and strong enforcement provisions, ideally an enforcement role for state attorneys general as well, or even private citizens.

Yes, so I think that the BROWSER Act could be strengthened for sure.

Mr. ENGEL. So you just said private citizens. Should Congress consider granting private citizens the right to bring civil actions against companies for violating privacy regulations?

Ms. MOY. I do think that if Congress is serious about ensuring that businesses actually adhere to the standards set forth in the statute, then a private right of action is one of the strongest enforcement mechanisms you can have to ensure that that takes place.

Mr. ENGEL. Now, rulemaking authority may help to protect consumer privacy but such protections still need to be enforced in order to be effective.

So let me ask you this: Do you think the FCC has done an adequate job of enforcing section 222 which establishes the duty of telecommunication carriers to protect the confidentiality of proprietary information?

Ms. MOY. I think that, at times, it has. It has not always been consistent, which is one of the reasons that it would be great to have additional enforcers, additional cops on the beat that can enforce those regulations.

In recent years, the FCC brought actions against four different carriers for CPNI violations, but since the change in administration, I don't believe there have been any.

Mr. ENGEL. Would more robust enforcement help fend off some of the abuses that have come to light recently such as what is happening with LocationSmart.

Ms. MOY. Certainly. I think we still haven't seen anything come out of the LocationSmart scandal. It could be one of the largest privacy violations that we have had in recent years, maybe as big as the the Facebook-Cambridge Analytica scandal, but all we have heard is crickets from the FCC.

Mr. ENGEL. Thank you. I see my time is up, Madam Chair. Thank you very much.

Mrs. BLACKBURN. I thank the gentleman.

Mr. Bilirakis, you are recognized.

Mr. BILIRAKIS. Thank you, Madam Chair.

I appreciate it very much. Mr. Haney as broadband was able to spread over the last 20 years, the rise of killer apps received a boost from the light-touch policies we put in motion. Gmail and Google Voice are two such services.

Gmail has been in the news recently as reports indicate that, even though Google said it would stop scanning the traffic, the company still permits software developers outside of Google to scan Gmail inboxes.

Google said that it only gives data to outside developers it has vetted. So it only gives data to outside developers it has vetted—again—and to whom users have granted permission to access email.

However, that still means software developers are able to review who sent an email, who it was sent to, the time sent, and the contents of the message itself, which might contain health information, financial records, or other sensitive personal information.

Is any of this information protected by the CPNI rules?

Mr. HANEY. No, sir, it is not.

Mr. BILIRAKIS. It is not.

Mr. HANEY. It is not. It doesn't relate to telephone calls that have actually called. It doesn't relate to duration of the telephone calls, the timing, or the phone numbers of the calls that were made. So CPNI would not apply to that situation.

Mr. BILIRAKIS. Thank you for answering me that.

Again, Mr. Haney, you mentioned a few times that often systems are burdensome and are reserved only for the most sensitive personal information.

Can you expand on the cost of the compliance with, again, the CPNI rules?

Mr. HANEY. I listed one example in my testimony. One of the telecommunications common carriers attempted to get opt-in approval across its subscriber base, and it was successful only 29 percent of the time or 29 percent of its customers. And the cost that incurred was over 20 dollars for every affirmative response that it got. And there are other studies that come up with, or other examples, other anecdotes that come up with simply results. Most of the time, consumers take no action. And this is verified because when they're offered the chance to opt out, very few choose to opt out.

And so I think the FTC is really, really on to something here by trying to categorize the most sensitive information that warrants the top, the highest protection, and, similarly, to try to identify more routine information, information that is not as sensitive, that doesn't require the most burdensome protection.

Mr. BILIRAKIS. OK. Very good. I think you answered my third question as well. So I appreciate it very much.

And I yield back, Madam Chair.

Mrs. BLACKBURN. The gentleman yields back.

At this time, I recognize Mr. Collins for 5 minutes.

Mr. COLLINS. Thank you, Madam Chair.

Thank you. When you have multiple hearings going on at once, here we go.

What I want to talk about, really, are the kinds of apps that we now know are being offered by various retailers in the name of giving you discounts, the frequent buyer program, or whatever. But we know that, in some ways, if you loaded that app onto your phone, all of a sudden, whether it is a Target or a Walmart or whomever, they may be able to track other information unknowingly.

So, Mr. Haney, I want to break this down a little bit. If you have such an app on your phone, you are in a retail establishment and you are going to use this, perhaps, for discounts or other things, can you talk about, a little bit, how that might work?

Mr. HANEY. Well, when I go to Home Depot, I believe my Home Depot app on my phone, it can tell me what aisle I'm looking for. It can tell where I am in the store, what store I'm in. I couldn't probably imagine every use that some of these brilliant people that are designing these apps, are contemplating. But the phones have multiple sensors in them, and apps can access some of the same information that other apps can access because it is stored in the operating system.

And as far as whether it is fair to expect consumers to anticipate all of the different uses, all of the different ways they can be tracked, I don't believe it is fair to expect them to anticipate that in every case.

But I do think that policymakers need to think in terms, not what agency has an office of engineering and what doesn't; we are talking about some very similar issues here. We are talking about irrespective of whether the underlying telecommunication services are being used for voice communication or an app that never connects with a Public Switched Network, we can always agree that what we are talking about is a voice communication.

And I think that, again, striving for uniformity and striving, if we are going to increase the baseline through regulation, anticipatory regulation, if we are going to increase that baseline, let's just really strive to make it the least burdensome that we possibly can, to not try to anticipate everything that the marketplace may dream up. Let them experiment a little bit. But it may be appropriate to increase the baseline.

Mr. COLLINS. I think that is all of our concerns. Everyone wants a discount, and you don't know what you don't know. And so, in this case, it could be your Wi-Fi; it could even be your microphone, certainly your GPS. And I think my concern would be, once you

leave the store, is that off? I know, on my phone, I have got an app—it asks me, do I want to keep my location open all the time, or do I want to have my location only working when I have activated it? And most folks don't even know how to turn that on or off. So we are all about protecting our consumers, but this technology is going way faster——

Mr. HANEY. Yes.

Mr. COLLINS [continuing]. Than anything we could imagine on the consumer protection front. We don't know what we don't know. So, I guess, Mr. McDowell, I guess you would agree most consumers don't anticipate or know the extent to which somebody could be tracking them.

Mr. MCDOWELL. First of all, I want to associate my remarks with Mr. Haney's just now. They were terrific.

Absolutely, we don't know what we don't know. We don't know what is coming over the horizon. So there is that balance between we want to make sure we have this robust experimental marketplace that I believe firmly brings us more benefits than harms, but it does bring us harms, and so what do we do about those as policymakers?

Mr. COLLINS. Well, I appreciate that. Sorry I was late, Madam Chair.

But I yield back and thank the witnesses for their testimony.

Mrs. BLACKBURN. The gentleman yields back.

And there are no other members at this point wishing to ask questions. So we appreciate all of you being here today.

Before we conclude this hearing, I ask unanimous consent to enter into the record the following documents: An article from Axios, an article from Fast Company on location tracking, an article from Ars Technica on call record scraping.

Without objection, so ordered.

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

Mrs. BLACKBURN. Pursuant to committee rules, I remind members that they have 10 business days to submit additional questions. And I ask the witnesses to submit their responses within 10 business days upon receipt of the questions.

Seeing no further business to come before the subcommittee today, and as you all see, there is agreement that we need to address the privacy and data security issues, without objection, the subcommittee is adjourned.

[Whereupon, at 1:25 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Good morning. As questions continue to arise surrounding the exchange between consumers and the technology platforms and services they use on a daily basis, the Energy and Commerce Committee has focused its attention on the protection, transparency, and use of consumer data. Earlier this week, Chairman Blackburn and I, along with Chairman Latta and Chairman Harper, sent letters to Apple and Google to inquire about their data collection and sharing practices.

We continue this important conversation today in the context of protecting customer proprietary network information, or CPNI. We can all recognize the importance of protecting consumers' personal information, no matter what kind of network they are using for communication.

In the decades since Congress enacted the Communications Act of 1996, requiring telecommunications carriers to protect the confidentiality of CPNI, the Federal Com-

munications Commission (FCC) has updated CPNI rules to address evolving technology, practices, and consumer expectations.

For example, in 2007, the FCC extended the CPNI rules to cover voice calls made over the IP network that interconnected with the traditional telephone network. At that time, the FCC also beefed up its authentication provisions under the CPNI rules so third parties could not fraudulently obtain access to protected consumer data.

Again, in 2013, consumer expectations and changes in technology led the FCC to extend CPNI protections to data collected on mobile devices under the direction or control of a telecommunications carrier.

These were important advancements, and reflected the seriousness attached to how a customer's sensitive information, such as location data, is managed. Location information when attached to a call that touches the telephone network is considered to be "call detail information" and is thus protected under the CPNI rules. But, increasingly, other entities are utilizing location data to provide services on a mobile device that may not cross the public switched telephone network.

New applications that rely on location-based services can be useful, efficient, and even potentially life-saving for consumers. We're hearing of new innovations in ride-sharing where an emergency button within an app will connect you with a 911 call center. There are new partnerships forming to share phone device location data directly to 911 public safety answering points, separate from and in addition to carrier location information.

However, consumers deserve to know that an app that collects location information from a mobile device might not have to abide by the same rules as a telecommunications provider, and that their location information might not be as secure.

While these entities are outside of the scope of the current CPNI rules, we must consider the entire internet ecosystem as we continue to work on comprehensive solutions. We have companies now that provide live communication, act as content producers and publishers, and aggregate data—all in one package—and the old rules just don't fit the today's paradigms.

That is why the FCC's 2016 broadband privacy order was the wrong policy; we knew it wouldn't increase protections. That is why the 2015 net neutrality order was the wrong policy; we knew it wouldn't facilitate an environment to incentivize the next generation of services to close the close the broadband divide and deliver consumers smart cities, telemedicine, distance learning, and more.

Today, we need to thoughtfully consider how effective the old protections under CPNI are in today's information sharing world.

I'd like to thank our witnesses for joining us today. I look forward to hearing from you and hearing your insights.

AXIOS

Axios Jul 5

Smart TVs are watching us now

A woman walking by Panasonic Smart TVs. Photo: Adam Berry/Getty Images

"How Smart TVs in Millions of U.S. Homes Track More Than What's on Tonight," by N.Y. Times' Sapna Maheshwari: "[D]ata companies have harnessed new technology to immediately identify what people are watching on internet-connected TVs, then using that information to send targeted advertisements to other devices in their homes."

Why it matters: "Samba TV[, one of those data companies,] has even offered advertisers the ability to base their targeting on whether people watch conservative or liberal media outlets and which party's presidential debate[s] they watched."

- "**Samba TV** has struck deals with roughly a dozen TV brands — including Sony, Sharp, TCL and Philips — to place its software on certain sets."

recognizing onscreen content.' But the screen, which contains the enable button, does not detail how much information Samba TV collects to make those recommendations."

- "**Samba TV** ... said at the end of 2016 that more than 90 percent of people opted in."
- "**Once enabled,** Samba TV can track nearly everything that appears on the TV on a second-by-second basis, essentially reading pixels to identify network shows and ads, as well as programs on Netflix and HBO and even video games played on the TV."

Show less

SMART TVS >

A message from Qualcomm

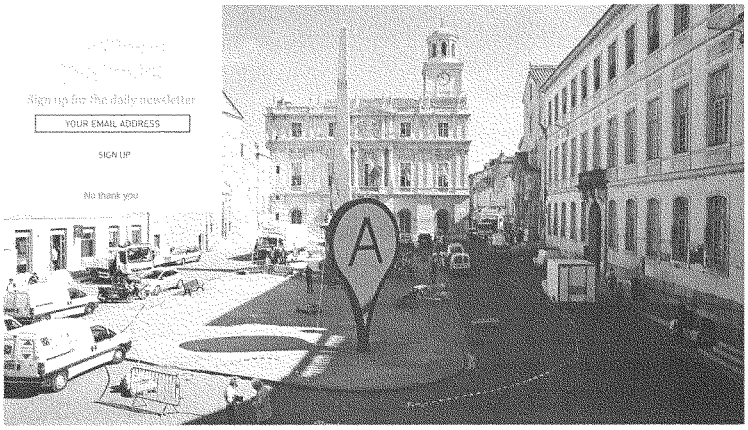
22 million more reasons 5G will change the world

Co.Design
Technology
Leadership
Entertainment
Ideas
Video
News

12.22.17

How—And Why—Apple, Google, And Facebook Follow You Around In Real Life

Big tech companies and others are quietly amassing mountains of users' location data, in ways many don't realize and sometimes can't avoid.



[Photo: Arambar/Wikipedia]

BY DJ PANGBURN
LONG READ

Even the most absent-minded smartphone user is probably aware that apps keep tabs on where they go. Many apps wouldn't work without location data. But few realize just how often that location tracking is happening—even when it's not necessary, even when their apps aren't being used, and, increasingly, even when a user isn't even carrying their phone. Tracking you across the map isn't always about improving user experience, of course, but rather about better understanding who you are and what kind of advertising to show you. If, for instance, a company knows that you've just stepped foot in one of their stores, they might start targeting you with ads touting a sale.

It's hard to dispute the value of a good sale, but location tracking raises all sorts of privacy concerns. (Not to mention that using the GPS will drain your smartphone's battery faster.) Should app makers know where we live, where our children go to school, where we go to get away from it all? And if so, how much should they tell us about it?

Those complicated questions help explain why the biggest tech companies, including Apple, Amazon, Facebook, Google, Twitter, and Verizon, filed a pro-privacy amicus brief in last month's Supreme Court case Carpenter v. United States, in which they argued that police should have a warrant before accessing cell phone location data. After all, if we thought the police could easily access our data, we might start asking more questions about what our phones know about us, and become less comfortable with using these companies' products.

But location tracking is quietly, sometimes surreptitiously, baked into the web's modern data collection regime. According to a recent study by French research organization Exodus Privacy and Yale University's Privacy Lab, more than three in four Android apps contain at least one third-party "tracker," which uses various techniques to glean personal information, including location and in-app behavior, to better target users for advertisements and services. (In 2016, the FTC sued InMobi, a company that described itself as "the world's largest independent mobile advertising company" because it tracked consumers' location even if they denied permission.)

The trackers found by the Yale researchers include some of the most popular apps on the Google Play Store, including Tinder, Spotify, Uber, and OKCupid. Many of these apps rely on a service owned by Google, Crashlytics, that primarily tracks app crash reports, but can also provide the ability to "get insight into your users, what they're doing, and inject live social content to delight them." The researchers didn't study iOS apps, but they warned that the problem may also exist on Apple's App Store, noting that many of the tracker companies used on Android apps also distribute apps via Apple.

ADVERTISING

Learn More

inRead invented by Teads

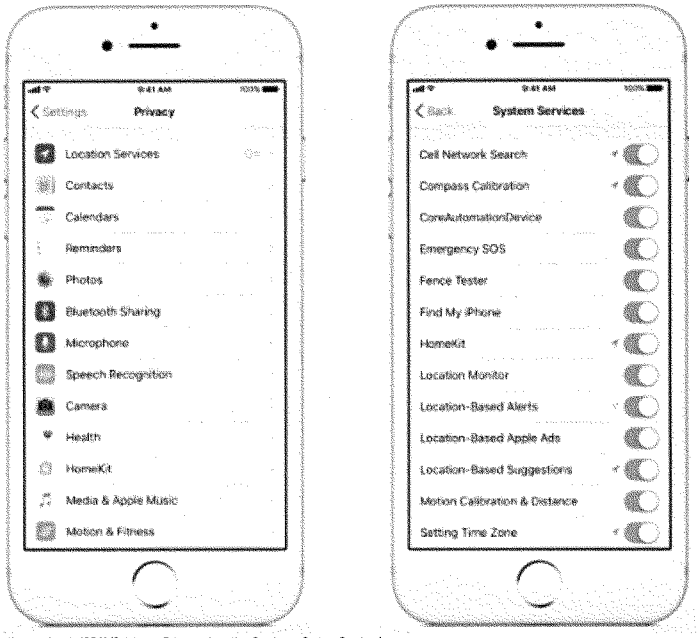
[Photo: Flickr user U.S. Department of Energy]

Even so-called anonymized location data—without our real-life name attached to it—can help paint a detailed portrait of a user and their habits, or even crack open their entire identity. Like the National Security Agency, which gathers billions of records a day on people's cell-phone locations across the globe, developers realize there is a lot to be gleaned from users' frequented locations and movement patterns. For app developers and ad targeters, this locational awareness is "the stuff of the future," as one data scientist put it to me recently. Here's how three of the largest companies are gathering your location, and what, if anything, you can do about it.

APPLE: "A BETTER USER EXPERIENCE" AND TARGETED ADS

The company has been lauded by some for its emphasis on privacy. As Apple chief executive Tim Cook says in a letter at the company's privacy webpage, "When we do ask to use your data, it's to provide you with a better user experience."

But Apple's handling of location data has faced criticism before. In 2011, Apple was found to be storing location data on users' phones in an unencrypted file; it subsequently encrypted that kind of data on the device, on the cloud, and in transit. And in a class-action lawsuit filed in 2014, plaintiff Chen Ma was concerned that, among other things, users were given "no meaningful" way to switch off Location Services without "substantially compromising" key parts of the iPhone's functionality.



Privacy and location services in iOS 11 (Settings > Privacy > Location Services > System Services).

Apple still collects a lot of location data, though it says it doesn't share this data directly with advertisers: Like Facebook and Google, it only makes your data available to them by putting you in an "anonymized" targeting group. iPhone users can turn off "Location-based Apple ads," thanks to a small radio button deep inside the settings app (Settings > Privacy > Location Services > System Services; even with that off, however, Apple still builds an ad targeting profile on you based on keyboard language settings, device type, App Store searches and Apple News articles you read, though some of that tracking can be limited under Settings > Privacy > Advertising.)

If Location Services is on, some location data collection can't be turned off at all. With Location Services enabled, according to Apple, "your device will periodically send the geo-tagged locations of nearby Wi-Fi hotspots and cell towers to Apple to augment Apple's crowd-sourced database of Wi-Fi hotspot and cell tower locations." If you're moving in a vehicle, "a GPS-enabled iOS device will also periodically send GPS locations and travel speed information to Apple to be used for building up Apple's crowd-sourced road-traffic database." (This "crowd-sourced location data" is "anonymous and encrypted," Apple adds. "It doesn't personally identify you.")

All of this location data is owned by Apple. At the very bottom of another page, Apple clarifies that by enabling Location Services for your devices, "you agree and consent to the transmission, collection, maintenance, processing, and use of your location data and location search queries by Apple, its partners, and licensees to provide and improve location-based and road traffic-based products and services." Most users have little choice here: As Chen Ma pointed out in her lawsuit, many apps simply can't function without activating location services in some form.

On iOS, navigate to Settings, then scroll down and tap on Privacy, then tap on Location Services. Users can disable location tracking wholesale by toggling the slider to off, or can control which specific apps have access to location and when. In iOS 11, users can choose to allow an app to track their location either "Never" or only while using the app.

GOOGLE: AN ARSENAL OF TOOLS TRACKS YOU ONLINE AND OFFLINE

Like Facebook and others, Google is working to insert itself even further into our daily transactions, and location data is critical to that. Google's fleet of apps—Gmail, Chrome, Gchat, and of course Maps—collect location data with user permission; other apps in the Android ecosystem also gather location data, sometimes without permission (see above). Like many other data companies, Google also follows users across the internet with web cookies that track IP addresses, which, as the *Guardian* reported last year, allows the service to make pretty informed guesses on user locations and habits.

The tech giant also uses what is known as "implicit location information," which is when Google interprets a search for a specific location ("Empire State building restaurants nearby," for instance) as evidence the person will be visiting the building; then targets related ads at the user based on this information.

In March, Google announced a new program aimed at tracking users' offline locations and behavior too, using data gathered from third-parties. (The company says it has access to about 70% of U.S. credit and debit card transactions through partnerships with data companies.) After a user clicks on a merchant's digital ad, Google can determine if that person purchased something in that merchant's bricks-and-mortar store; that could help persuade merchants to spend more on ads. At the time, Google said it would "match transactions back to Google ads in a secure and privacy-safe way, and only report on aggregated and anonymized store sales to protect your customer data."

Google has also managed to collect user locations in more surreptitious ways. As *Quartz* reported last month, Google collected the physical addresses of nearby cell towers with which Android users' phones were communicating for everyday text, call and app usage. Gathering data from several cell towers effectively allows Google to triangulate a user's cell signal, and thus determine an approximate location—even when users have location services turned off or have removed their SIM card. Google told *Quartz* that this data was not stored, and that it would end the data collection.

To disable location tracking on an Android device, go to Settings, scroll down and tap Location, then switch the slider to the off position. However, as with iOS apps (above), this will turn off all location tracking so that apps like Google Maps or even Uber or Lyft won't work. To control location tracking with more granularity, go into each app through the App Manager and turn off location tracking. Android Users can also view and delete their device's location history. All users of Google services can also see their location data through the company's Timeline page, and can opt out of having some of their activities logged and opt out of being shown some ads.

Related: The Popular Design Tool That's Actually A Privacy Nightmare

FACEBOOK CAN ALSO TELL WHERE YOU SHOP OFFLINE

As with other smartphone apps, Facebook, Messenger, WhatsApp, and Instagram also attempt to capture your location across devices and throughout the course of the day, from your early-morning reading habits, to a Spotify playlist during your commute, to your social media browsing at night. Like Google, Facebook wants to help advertisers know if their ads led you to visit the advertisers' brick-and-mortar store, and to help "retarget" ads at you if you have. You don't need to be online, or with your device either: Facebook, like Google and other large data gatherers, are also determined to link not just your online locations and data, but your offline location data too.

As of September, advertisers can use Facebook data as well as custom data provided by the advertiser, like a list of in-store purchases, to target ads at users. "This feature allows businesses to re-engage in-store audiences with more relevant and compelling campaigns, as well as create lookalike audiences," Facebook said in a statement. An apparel brand could "choose to exclude in-store customers, for example, when running a promotion available only for new customers."

To turn off location tracking for Facebook, see its explainer, and check your privacy settings to choose how the platform targets ads at you. Note that you can't stop someone like a friend from tagging your location or your Facebook profile in a location-tagged photo. It's also worth mentioning that if you upload a photo to Facebook, unless you've disabled location tracking, the photo will include geotags that provide Facebook with location data on where the photo was taken. To see your check-in locations, from your profile, hover your mouse over "More" and click "Check-ins." Users can also download their Facebook data to see login locations.

In general, it's also a good idea to routinely clear your browser of cookies and trackers that Facebook and other companies use to track you in digital and physical space.

Related: Here's How To Track The Smartphone Apps That Are Tracking You

HOW WHATSAPP AND INSTAGRAM FEED FACEBOOK'S LOCATION DATABASE

Some apps are less obvious about their location tracking. Take WhatsApp, the popular Facebook-owned messaging app that lets users communicate with encryption via Wi-Fi instead of on their cellular data plans. On the surface, it would seem that WhatsApp wouldn't require location data. But I recently noticed that location services were enabled on my iPhone's WhatsApp app. Based on my frequency of usage, this means that WhatsApp was pretty much always tracking my location for the last seven months, and feeding that data into the internal profile Facebook uses to track me. Facebook uses Instagram data in a similar way.

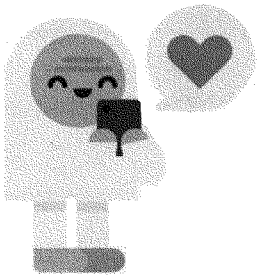
In November 2016, after protests and pressure from privacy regulators in Europe over Facebook's decision to combine WhatsApp data with Facebook data, the social media platform temporarily paused its data sharing program for European users. In May, the European Commission fined Facebook $122 million for misleading WhatsApp users about its data sharing with Facebook.

NEW PHONE, WHO DIS —

Facebook scraped call, text message data for years from Android phones [Updated]

Maybe check your data archive to see if Facebook's algorithms know who you called.

SEAN GALLAGHER - 3/24/2018, 6:20 PM



SUBSCRIPTIONS SIGN IN

Continuously upload info about your contacts like phone numbers and nicknames, and your call and text history. This lets friends find each other on Facebook and helps us create a better experience for everyone. Learn More.

Facebook

Enlarge / This screen in the Messenger application offers to conveniently track all your calls and messages. But Facebook was already doing this surreptitiously on some Android devices until October 2017, exploiting the way an older Android API handled permissions.

[Update, March 25, 2018, 20:24 Eastern Time]: Facebook has responded to this and other reports regarding the collection of call and SMS data with a blog post that denies Facebook

reports regarding the collection of call and SMS data with a blog post that denies Facebook collected call data surreptitiously. The company also writes that it never sells the data and that users are in control of the data uploaded to Facebook. This "fact check" contradicts several details Ars found in analysis of Facebook data downloads and testimony from users who provided the data. More on the Facebook response is appended to the end of the original article below.

This past week, a New Zealand man was looking through the data Facebook had collected from him in an archive he had pulled down from the social networking site. While scanning the information Facebook had stored about his contacts, Dylan McKay discovered something distressing: Facebook also had about two years' worth of phone call metadata from his Android phone, including names, phone numbers, and the length of each call made or received.

14:53 UTC+13

Number:+61223[redacted]

Call Type	Start time	Duration	Name	Number Label
OUTGOING	Monday, 28 November 2016 at 21:57 UTC+13	2	Mereana Gell	
OUTGOING	Sunday, 16 April 2017 at 10:53 UTC+12	42	Mereana Gell	
MISSED	Monday, 13 February 2017 at 18:18 UTC+13	0	Mereana Gell	
OUTGOING	Tuesday, 29 November 2016 at 17:09 UTC+13	446	Mereana Gell	
INCOMING	Sunday, 26 March 2017 at 11:33 UTC+13	120	Mereana Gell	
OUTGOING	Sunday, 26 March 2017 at 12:37 UTC+13	115	Mereana Gell	
INCOMING	Saturday, 6 May 2017 at	39	Mereana Gell	

Dylan McKay
@dylanmckaynz

Downloaded my facebook data as a ZIP file

Somehow it has my entire call history with my partner's mum

4:04 AM - Mar 21, 2018

52.3K 41.7K people are talking about this

This experience has been shared by a number of other Facebook users who spoke with Ars, as well as independently by us—my own Facebook data archive, I found, contained call-log data for a certain Android device I used in 2015 and 2016, along with SMS and MMS message metadata.

Calls I made to my office number to check my voicemail, and from my office number to find my phone, found in my Facet archive. In total, there were two years of call data, from the period I used my Blackphone as my primary phone.

In response to an email inquiry by Ars about this data gathering, a Facebook spokesperson replied, "The most important part of apps and services that help you make connections is to make it easy to find the people you want to connect with. So, the first time you sign in on your phone to a messaging or social app, it's a widely used practice to begin by uploading your phone contacts."

The spokesperson pointed out that contact uploading is optional and installation of the application explicitly requests permission to access contacts. And users can delete contact data from their profiles using a tool accessible via Web browser.

Facebook uses phone-contact data as part of its friend recommendation algorithm. And in recent versions of the Messenger application for Android and Facebook Lite devices, a more explicit request is made to users

FURTHER READING
Facebook's Cambridge Analytica scandal, explained [Updated]

for access to call logs and SMS logs on Android and Facebook Lite devices. But even if users didn't give that permission to Messenger, they may have given it inadvertently for years through Facebook's mobile apps—because of the way Android has handled permissions for accessing call logs in the past. (For Facebook's instructions on turning off continuous contact uploading, go here.)

If you granted permission to read contacts during Facebook's installation on Android a few versions ago—specifically before Android 4.1 (Jelly Bean)—that permission also granted Facebook access to call and message logs by default. The permission structure was changed in the Android API in version 16. From Android 4.1 on, a single request from those applications would trigger two separate permission requests.

But until the "Marshmallow" version of Android, even with split permissions, all permissions could still be presented all at once, without users getting the option to decline them individually. So Facebook and other applications could continue to gain access to call and SMS data with a single request by specifying an earlier Android SDK version. Starting with Marshmallow, users could toggle these permissions separately themselves. But as many as half of Android users worldwide remain on older versions of the operating system because of carrier restrictions on updates or other issues.

Apple iOS has never allowed access to call log data by third-party apps, overt or silently, so this sort of data acquisition was never possible.

Facebook provides a way for users to purge collected contact data from their accounts, but it's not clear if this deletes just contacts or if it also purges call and SMS metadata. After purging my contact data, my contacts and calls were still in the archive I downloaded the next day—likely because the archive was not regenerated for my new request. (**Update:** The cached archive was generated once and not updated on the second request. However, two days after a request to delete all contact data, the contacts were still listed by the contact management tool.)

As always, if you're really concerned about privacy, you should not share address book and call-log data with any mobile application. And you may want to examine the rest of what can be found in the downloadable Facebook archive, as it includes all the advertisers that Facebook has shared your contact information with, among other things.

Update, March 25, 2018, continued:

Facebook responded to reports that it collected phone and SMS data without users' knowledge in a "fact check" blog post on Sunday. In the response, a Facebook spokesperson stated:

> Call and text history logging is part of an opt-in feature for people using Messenger or Facebook Lite on Android. This helps you find and stay connected with the people you care about, and provide you with a better experience across Facebook. People have to expressly agree to use this feature. If, at any time, they no longer wish to use this feature they can turn it off in settings, or here for Facebook Lite users, and all previously shared call and text
>
> history shared via that app is deleted. While we receive certain permissions from Android, uploading this information has always been opt-in only.

This contradicts the experience of several users who shared their data with Ars. Dylan McKay told Ars that he installed Messenger in 2015, but only allowed the app the permissions in the Android manifest that were required for installation. He says he removed and reinstalled the app several

manifest that were required for installation. He says he removed and reinstalled the app several times over the course of the next few years, but never explicitly gave the app permission to read his SMS records and call history. McKay's call and SMS data runs through July of 2017.

In my case, a review of my Google Play data confirms that Messenger was never installed on the Android devices I used. Facebook was installed on a Nexus tablet I used and on the Blackphone 2 in 2015, and there was never an explicit message requesting access to phone call and SMS data. Yet there is call data from the end of 2015 until late 2016, when I reinstalled the operating system on the Blackphone 2 and wiped all applications.

While data collection was technically "opt-in," in both these cases the opt-in was the default installation mode for Facebook's application, not a separate notification of data collection. Facebook never explicitly revealed that the data was being collected, and it was only discovered as part of a review of the data associated with the accounts. The users we talked to only performed such reviews after the recent revelations about Cambridge Analytica's use of Facebook data.

Facebook began explicitly asking permission from users of Messenger and Facebook Lite to access SMS and call data to "help friends find each other" after being publicly shamed in 2016 over the way it handled the "opt-in" for SMS services. That message mentioned nothing about retaining SMS and call data, but instead it offered an "OK" button to approve "keeping all of your SMS messages in one place."

Facebook says that the company keeps the data secure and does not sell it to third parties. But the post doesn't address why it would be necessary to retain not just the numbers of contacts from phone calls and SMS messages, but the date, time, and length of those calls for years.

READER COMMENTS 342 SHARE THIS STORY

SEAN GALLAGHER

Sean is Ars Technica's IT and National Security Editor. A former Navy officer, systems administrator, and network systems integrator with 20 years of IT journalism experience, he lives and works in Baltimore, Maryland.

EMAIL sean.gallagher@arstechnica.com // **TWITTER** @thepacketrat

Unsolved mysteries of League of Legend:

WATCH

Chris Hadfield