

**FACEBOOK: TRANSPARENCY AND USE OF  
CONSUMER DATA**

---

---

**HEARING**  
BEFORE THE  
**COMMITTEE ON ENERGY AND  
COMMERCE**  
**HOUSE OF REPRESENTATIVES**  
ONE HUNDRED FIFTEENTH CONGRESS  
SECOND SESSION

APRIL 11, 2018

**Serial No. 115-114**



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

U.S. GOVERNMENT PUBLISHING OFFICE

30-956 PDF

WASHINGTON : 2018

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 LUJAN, New Mexico

PAUL TONKO, New York

YVETTE D. CLARKE, New York

DAVID LOEBSACK, Iowa

KURT SCHRAEDER, Oregon

JOSEPH P. KENNEDY, III, Massachusetts

TONY CARDENAS, California

RAUL RUIZ, California

SCOTT H. PETERS, California

DEBBIE DINGELL, Michigan

## C O N T E N T S

---

	Page
Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement .....	2
Prepared statement .....	4
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement .....	5
Prepared statement .....	6

### WITNESS

Mark Zuckerberg, Cofounder, Chairman, and Chief Executive Officer, Facebook, Inc. ....	8
Prepared statement .....	10
Answers to submitted questions <sup>1</sup> .....	212

### SUBMITTED MATERIAL

Subcommittee memorandum .....	106
Article of November 20, 2012, “Friended: How the Obama Campaign Con- nected with Young Voters,” by Michael Scherer, Time, submitted by Mr. Burgess .....	112
Article of April 9, 2018, “We Already Know How to Protect Ourselves From Facebook,” by Zeynep Tufekci, New York Times, submitted by Mr. Burgess .	114
Article of March 21, 2018, “It’s Time to Break Up Facebook,” by Eric Wilson, Politico, submitted by Mr. Burgess .....	118
Letter of April 9, 2018, from Faiz Shakir, National Political Director, and Neema Singh Guliani, Legislative Counsel, American Civil Liberties Union, to Representatives in Congress, submitted by Mr. Walden .....	120
Statement of NetChoice by Carl Szabo, Vice President and General Counsel, April 9, 2018, submitted by Mr. Walden .....	125
Letter of April 5, 2018, from John Rowan, National President and Chief Executive Officer, Vietnam Veterans of America, to Mr. Walden and Mr. Pallone, submitted by Mr. Walden .....	131
Letter of April 11, 2018, from Allison S. Bohm, Policy Counsel, Public Knowl- edge, to Mr. Walden and Mr. Pallone, submitted by Mr. Walden .....	142
Letter of April 10, 2018, from Marc Rotenberg, President, Electronic Privacy Information Center, et al., to House Energy and Commerce Committee members, submitted by Mr. Walden .....	147
Federal Trade Commission Complaint of December 17, 2009, by Marc Rotenberg, President, Electronic Privacy Information Center, et al., sub- mitted by Mr. Walden .....	163
Letter of April 10, 2018, from Charles H. Rivkin, Chairman and Chief Execu- tive Officer, Motion Picture Association of America, to Mr. Walden and Mr. Pallone, submitted by Mr. Walden .....	192
Letter of April 10, 2018, from Morgan Reed, President, ACT, the App Associa- tion, to Mr. Walden and Mr. Pallone, submitted by Mr. Walden .....	193
Letter of April 10, 2018, from Curt Levey, President, and Ashley Baker, Director of Public Policy, the Committee for Justice, to Mr. Walden and Mr. Pallone, submitted by Mr. Walden .....	201

<sup>1</sup> Questions for the record and responses from Facebook, Inc., have been retained in committee files and also are available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108090>.

IV

	Page
Letter of April 9, 2018, from Jeffrey Chester, U.S. Co-Chair, and Finn Lützow-Holm Myrstad, EU Co-Chair, Digital Policy Committee, Trans Atlantic Consumer Dialogue, to Mark Zuckerberg, Chief Executive Officer, Facebook, submitted by Mr. Walden .....	205
Letter of October 30, 2017, from Arab American Institute, et al., to Mark Zuckerberg, Chief Executive Officer, and Sheryl Sandberg, Chief Operating Officer, Facebook, submitted by Mr. Walden .....	206
Statement of National Council of Negro Women by Janice L. Mathis, Executive Director, April 10, 2018, submitted by Mr. Walden .....	211

## **FACEBOOK: TRANSPARENCY AND USE OF CONSUMER DATA**

**WEDNESDAY, APRIL 11, 2018**

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ENERGY AND COMMERCE,  
WASHINGTON, DC.

The committee met, pursuant to call, at 9:59 a.m., in room 2123, Rayburn House Office Building, Hon. Greg Walden (chairman of the committee) presiding.

Members present: Representatives Walden, Barton, Upton, Shimkus, Burgess, Blackburn, Scalise, Latta, McMorris Rodgers, Harper, Lance, Guthrie, Olson, McKinley, Kinzinger, Griffith, Bilirakis, Johnson, Long, Bucshon, Flores, Brooks, Mullin, Hudson, Collins, Cramer, Walberg, Walters, Costello, Carter, Duncan, Pallone, Rush, Eshoo, Engel, Green, DeGette, Doyle, Schakowsky, Butterfield, Matsui, Castor, Sarbanes, McNerney, Welch, Luján, Tonko, Clarke, Loeb sack, Schrader, Kennedy, Cárdenas, Ruiz, Peters, and Dingell.

Staff present: Jon Adame, Policy Coordinator, Communications and Technology; Mike Bloomquist, Staff Director; Daniel Butler, Staff Assistant; Karen Christian, General Counsel; Kelly Collins, Legislative Clerk, Energy/Environment; Zack Dareshori, Legislative Clerk, Health; Jordan Davis, Director of Policy and External Affairs; Melissa Froelich, Chief Counsel, Digital Commerce and Consumer Protection; Adam Fromm, Director of Outreach and Coalitions; Ali Fulling, Legislative Clerk, Oversight and Investigations, Digital Commerce and Consumer Protection; Theresa Gambo, Human Resources and Office Administrator; Brighton Haslett, Counsel, Oversight and Investigations; Elena Hernandez, Press Secretary; Zach Hunter, Communications Director; Paul Jackson, Professional Staff Member, Digital Commerce and Consumer Protection; Peter Kiely, Deputy General Counsel; Bijan Koohmaraie, Counsel, Digital Commerce and Consumer Protection; Ryan Long, Deputy Staff Director; Milly Lothian, Press Assistant and Digital Coordinator; Mark Ratner, Policy Coordinator; Austin Stonebraker, Press Assistant; Evan Viau, Legislative Clerk, Communications and Technology; Hamlin Wade, Special Advisor for External Affairs; Everett Winnick, Director of Information Technology; Greg Zerzan, Counsel, Digital Commerce and Consumer Protection; Michelle Ash, Minority Chief Counsel, Digital Commerce and Consumer Protection; Julie Babayan, Minority Counsel; Jeff Carroll, Minority Staff Director; Jennifer Epperson, Minority FCC Detailee; David Goldman, Minority Chief Counsel, Communications and Technology; Lisa Goldman, Minority Counsel; Tiffany Guarascio,

Minority Deputy Staff Director and Chief Health Advisor; Zach Kahan, Minority Outreach and Member Services Coordinator; Jerry Leverich III, Minority Counsel; Dan Miller, Minority Policy Analyst; Caroline Paris-Behr, Minority Policy Analyst; Kaitlyn Peel, Minority Digital Director; Tim Robinson, Minority Chief Counsel; Michelle Rusk, Minority FTC Detailee; Andrew Souvall, Minority Director of Communications; and C.J. Young, Minority Press Secretary.

Mr. WALDEN. The Committee on Energy and Commerce will now come to order.

Before my opening statement, just as a reminder to our committee members on both sides, it is another busy day at Energy and Commerce. In addition, as you will recall, to this morning's Facebook hearing, later today our Health Subcommittee will hold its third in the series of legislative hearings on solutions to combat the opioid crisis. And remember, our Oversight and Investigations Subcommittee will hold a hearing where we will get an update on the restoration of Puerto Rico's electric infrastructure following last year's hurricane season.

So, just a reminder, when this hearing concludes, I think we have votes on the House floor. Our intent is to get through every Member before that point to be able to ask questions, but then after the votes, we will come back into our subcommittees to do that work. As Ray Baum used to say, the fun never stops.

The Chair now recognizes himself for 5 minutes for purposes of an opening statement.

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

Good morning. Welcome, Mr. Zuckerberg, to the Energy and Commerce Committee in the House. We have called you here today for two reasons: One is to examine the alarming reports regarding breaches of trust between your company, one of the biggest and most powerful in the world, and its users; and the second reason is to widen our lens to larger questions about the fundamental relationship tech companies have with their users.

The incident involving Cambridge Analytica and the compromised personal information of approximately 87 million American users—or mostly American users—is deeply disturbing to this committee.

The American people are concerned about how Facebook protects and profits from its users' data. In short, does Facebook keep its end of the agreement with its users? How should we as policymakers evaluate and respond to these events?

Does Congress need to clarify whether or not consumers own or have any real power over their online data? Have edge providers grown to the point that they need Federal supervision?

You and your cofounders started a company in your dorm room that has grown to be one of the biggest and most successful businesses in the entire world. Through innovation and quintessentially American entrepreneurial spirit, Facebook and the tech companies that have flourished in Silicon Valley join the legacy of great American companies who build our Nation, drove our economy forward, and created jobs and opportunity. And you did it

all without having to ask permission from the Federal Government and with very little regulatory involvement.

The company you created disrupted entire industries and has become an integral part of our daily lives. Your success story is an American success story, embodying our shared values of freedom of speech, freedom of association, and freedom of enterprise.

Facebook also provides jobs for thousands of Americans, including my own congressional district, with data centers in Prineville. Many of our constituents feel a genuine sense of pride and gratitude for what you have created, and you are rightly considered one of the era's greatest entrepreneurs.

This unparalleled achievement is why we look to you with a special sense of obligation and hope for deep introspection. While Facebook has certainly grown, I worry it may not have matured. I think it is time to ask whether Facebook may have moved too fast and broken too many things.

There are critical unanswered questions surrounding Facebook's business model and the entire digital ecosystem regarding online privacy and consumer protection: What exactly is Facebook? Social platform? A data company? An advertising company? A media company? A common carrier in the information age? All of the above or something else?

Users trust Facebook with a great deal of information: their name, hometown, email, phone number, photos, private messages, and much, much more. But in many instances, users are not purposely providing Facebook with data. Facebook collects this information while users simply browse other websites, shop online, or use a third-party app.

People are willing to share quite a bit about their lives online based on the belief they can easily navigate and control privacy settings and trust that their personal information is in good hands. If a company fails to keep its promises about how personal data are being used, that breach of trust must have consequences.

Today we hope to shed light on Facebook's policies and practices surrounding third-party access to and use of user data. We also hope you can help clear up the considerable confusion that exists about how people's Facebook data are used outside of the platform.

We hope you can help Congress, but more importantly the American people, better understand how Facebook user information has been accessed by third parties from Cambridge Analytica and Cubeyou to the Obama for America Presidential campaign.

And we ask that you share any suggestions you have for ways policymakers can help reassure our constituents that data they believe was only shared with friends or certain groups remains private to those circles. As policymakers, we want to be sure that consumers are adequately informed about how their online activities and information are used.

These issues apply not just to Facebook but equally to the other internet-based companies that collect information about users online.

So, Mr. Zuckerberg, your expertise in this field is without rival. So thank you for joining us today to help us learn more about these vital matters and to answer our questions.

[The prepared statement of Mr. Walden follows:]

## PREPARED STATEMENT OF HON. GREG WALDEN

Good morning and welcome, Mr. Zuckerberg, to the Energy and Commerce Committee.

We've called you here today for two reasons: One is to examine alarming reports regarding breaches of trust between your company—one of the biggest and most powerful in the world—and its users. And the second reason is to widen our lens to larger questions about the fundamental relationship between tech companies and their users.

The incident involving Cambridge Analytica and the compromised personal information of approximately 87 million users, mostly Americans, is deeply disturbing to this committee.

The American people are concerned about how Facebook protects and profits from its users' data. In short, does Facebook keep its end of the agreement with its users? How should we, as policy makers, evaluate and respond to these events?

Does Congress need to clarify whether or not consumers own or have any real power over their online data? Have edge providers grown to the point that they need Federal supervision?

You and your co-founders started a company in your dorm room that has grown to be one of the biggest and most successful businesses in the world. Through innovation and a quintessentially American entrepreneurial spirit, Facebook and the tech companies that have flourished in Silicon Valley join a legacy of great American companies who built our Nation, drove our economy forward, and created jobs and opportunity. And you did it all without having to ask permission from the Federal Government, and with very little regulatory involvement. The company you created disrupted entire industries and has become an integral part of our lives.

Your success story is an American success story, embodying our shared values of freedom of speech, freedom of association, and freedom of enterprise. Facebook also provides jobs for thousands of Americans, including in my own congressional district at the data center in Prineville, Oregon. Many of our constituents feel a genuine sense of pride and gratitude for what you have created, and you are rightly considered one of this era's greatest entrepreneurs.

This unparalleled achievement is why we look to you with a special sense of obligation and hope for deep introspection.

While Facebook has certainly grown, I worry it has not matured. I think it is time to ask whether Facebook may have moved too fast and broken too many things.

There are critical, unanswered questions surrounding Facebook's business model and the entire digital ecosystem regarding online privacy and consumer protection.

What exactly is Facebook—a social platform, a data company, an advertising company, a media company, a common carrier in the information age, all of the above, or something else?

Users trust Facebook with a great deal of information—their name, hometown, email, phone number, photos, private messages, and much, much more. But in many instances, users aren't actively providing Facebook with data. Facebook collects this information while users simply browse other websites, shop online, or use a third-party app.

People are willing to share quite a bit about their lives online based on the belief that they can easily navigate and control privacy settings and trust that their personal information is in good hands.

If a company fails to keep its promises about how personal data are being used, that breach of trust must have consequences.

Today, we hope to shed light on Facebook's policies and practices surrounding third-party access to and use of user data. We also hope you can help clear up the considerable confusion that exists about how people's Facebook data are used outside the platform.

We hope you can help Congress, but more importantly the American people, better understand how Facebook user information has been accessed by third parties, from Cambridge Analytica and CubeYou, to the Obama for America presidential campaign.

And we ask that you share any suggestions you have for ways policymakers can help reassure our constituents that data they believe was only shared with friends or certain groups, remains private to those circles.

As policymakers we want to be sure that consumers are adequately informed about how their online activities and information are used. These issues apply not just to Facebook, but equally to the other internet-based companies that collect information about users online.

Mr. Zuckerberg, your expertise in this field is without rival. Thank you for joining us today to help us learn more about these vital matters.



And now, I yield to the gentleman from New Jersey, ranking member of the Energy and Commerce Committee Mr. Pallone, for 5 minutes.

Mr. WALDEN. With that, I yield now to the gentleman from New Jersey, the ranking member of the Energy and Commerce Committee, my friend Mr. Pallone, for 5 minutes for purposes of an opening statement.

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

Mr. PALLONE. Thank you, Mr. Chairman.

And I also want to thank you, Mr. Zuckerberg, for being here today.

Facebook has become integral to our lives. We don't just share pictures of our families. We use it to connect for school, to organize events, and to watch baseball games. Facebook has enabled everyday people to spur national political movements. Most of us in Congress use Facebook to reach our constituents in ways that were unimaginable 10 years ago, and this is certainly a good thing.

But it also means that many of us can't give it up easily. Many businesses have their only web presence on Facebook. And for professions like journalism, people's jobs depend on posting on the site.

And this ubiquity comes with a price. For all the good it brings, Facebook can be a weapon for those like Russia and Cambridge Analytica that seek to harm us and hack our democracy.

Facebook made it too easy for a single person—in this instance, Aleksandr Kogan—to get extensive personal information about 87 million people. He sold this data to Cambridge Analytica who used it to try to sway the 2016 Presidential election for the Trump campaign. And Facebook made itself a powerful tool for things like voter suppression, in part by opening its platform to app developers with little or no oversight.

But it gets worse. The fact is no one knows how many people have access to the Cambridge Analytica data, and no one knows how many other Cambridge Analyticas are still out there. Shutting down access to data to third parties isn't enough, in my opinion. Facebook and many other companies are doing the same thing: they are using people's personal information to do highly targeted product and political advertising.

And Facebook is just the latest in a never-ending string of companies that vacuum up our data but fail to keep it safe. And this incident demonstrates yet again that our laws are not working.

Making matters worse, Republicans here in Congress continue to block or even repeal the few privacy protections we have. In this era of nonstop data breaches, last year, Republicans eliminated existing privacy and data security protections at the FCC, and their justification was that those protections were not needed because the Federal Trade Commission has everything under control. Well, this latest disaster shows just how wrong the Republicans are.

The FTC used every tool Republicans have been willing to give it, and those tools weren't enough. And that is why Facebook acted like so many other companies and reacted only when it got bad press.

We all know this cycle by now: Our data is stolen. The company looks the other way. Eventually, reporters find out, publish a negative story, and the company apologizes. And Congress then holds a hearing, and then nothing happens.

By not doing its job, this Republican-controlled Congress has become complicit in this nonstop cycle of privacy by press release. And this cycle must stop because the current system is broken.

So I was happy to hear that Mr. Zuckerberg conceded that his industry needs to be regulated, and I agree. We need comprehensive privacy and data security legislation. We need baseline protections that stretch from internet service providers to data brokers to app developers and to anyone else who makes a living off our data. We need to figure out how to make sure these companies act responsibly even before the press finds out.

But while securing our privacy is necessary, it is not sufficient. We need to take steps immediately to secure our democracy. We can't let what happened in 2016 happen again, and to do that, we need to learn how Facebook was caught so flat-footed in 2016. How was it so blind to what the Russians and others were doing on its systems? Red flags were everywhere. Why didn't anyone see them, or were they ignored?

So today's hearing is a good start. But we also need to hold additional hearings where we hold accountable executives from other tech companies, internet service providers, data brokers, and anyone else that collects our information.

Now, Congresswoman Schakowsky from Illinois and I introduced a bill last year that would require companies to implement baseline data security standards, and I plan to work with my colleagues to draft additional legislation.

But I have to say, Mr. Chairman, it is time for this committee and this Congress to pass comprehensive legislation to prevent incidents like this in the future. My great fear is that we have this hearing today; there is a lot of press attention—and, Mr. Zuckerberg, you know, appreciate you being here once again, but if all we do is have a hearing and then nothing happens, then that is not accomplishing anything.

And, you know, I know I sound very critical of the Republicans and their leadership on this—on these privacy issues, but I have just seen it over and over again that we have the hearings and nothing happens. So excuse me for being so pessimistic, Mr. Chairman, but that is where I am.

I yield back.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Thank you for being here today, Mr. Zuckerberg.

Facebook has become integral to our lives. We don't just share pictures of our families. We use it to connect for school, to organize events, and to watch baseball games.

Facebook has enabled everyday people to spur national political movements. Most of us in Congress use Facebook to reach our constituents in ways that were unimaginable 10 years ago. This is a good thing.

But it also means that many of us can't give it up easily. Many businesses have their only web presence on Facebook. For professions like journalism, people's jobs depend on posting on the site.

This ubiquity comes with a price. For all the good it brings, Facebook can be a weapon for those like Russia and Cambridge Analytica that seek to harm us and hack our democracy.

Facebook made it too easy for a single person, in this instance Aleksandr Kogan, to get extensive personal information about 87 million people. Kogan then sold this data to Cambridge Analytica who used it to try to sway the 2016 Presidential election for the Trump Campaign. Facebook made itself a powerful tool for things like voter suppression in part by opening its platform to app developers with little or no oversight.

But it gets worse. The fact is no one knows how many people have access to the Cambridge Analytica data. And no one knows how many other Cambridge Analyticas are still out there.

Shutting down access to data to third parties isn't enough. Facebook and many other companies are doing the same thing. They are using people's personal information to do highly targeted product and political advertising.

And Facebook is just the latest in a never-ending string of companies that vacuum up our data but fail to keep it safe. This incident demonstrates yet again that our laws are not working.

Making matters worse, Republicans here in Congress continue to block or even repeal the few privacy protections we have. In this era of nonstop data breaches, last year Republicans eliminated existing privacy and data security protections at the Federal Communications Commission.

Their justification: those protections were not needed because the Federal Trade Commission has everything under control. Well this latest disaster shows just how wrong they are. The FTC used every tool Republicans have been willing to give it and those tools weren't enough.

That's why Facebook acted like so many other companies and reacted only when it got bad press. We all know the cycle by now: our data is stolen and the company looks the other way; eventually reporters find out, publish a negative story, and the company apologizes. Congress then holds a hearing; and then nothing.

By not doing its job, this Republican-controlled Congress has become complicit in this nonstop cycle of privacy by press release.

This cycle must stop because the current system is broken.

I was happy to hear Mr. Zuckerberg concede that his industry needs to be regulated. I agree.

We need comprehensive privacy and data security legislation.

We need baseline protections that stretch from internet service providers to data brokers to app developers and to anyone else who makes a living off our data.

We need to figure out how to make sure these companies act responsibly even before the press finds out.

But while securing our privacy is necessary, it's not sufficient. We need to take steps immediately to secure our democracy. We can't let what happened in 2016 happen again. To do that, we need to learn how Facebook was caught so flatfooted in 2016. How was it so blind to what the Russians and others were doing on its systems? Red flags were everywhere-why didn't anyone see them? Or were they ignored?

So today's hearing is a good start. But we also need to hold additional hearings where we hold accountable executives from other tech companies, internet service providers, data brokers, and anyone else that collects our information.

Congresswoman Schakowsky and I introduced a bill last year that would require companies to implement baseline data security standards, and I plan to work with my colleagues to draft additional legislation. It's time for this committee and this Congress to pass comprehensive legislation to prevent incidents like this in the future.

Mr. WALDEN. I think I thank the gentleman for his opening comments.

With that, we now conclude with Member opening statements. The Chair would like to remind Members that, pursuant to the committee rules, all Members' opening statements will be made part of the record.

Today we have Mr. Mark Zuckerberg, chairman and CEO of Facebook, Incorporated, here to testify before the full Energy and Commerce Committee. Mr. Zuckerberg will have the opportunity to

give a 5-minute opening statement followed by a round of questioning from our Members.

So thank you for taking the time to be here, and you are now recognized for 5 minutes.

**STATEMENT OF MARK ZUCKERBERG, COFOUNDER,  
CHAIRMAN AND CEO, FACEBOOK, INC.**

Mr. ZUCKERBERG. Thank you.

Chairman Walden, Ranking Member Pallone, and members of the committee, we face a number of important issues around privacy, security, and democracy, and you will rightfully have some hard questions for me to answer. Before I talk about the steps we are taking to address them, I want to talk for a minute about how we got there.

Facebook is an idealistic and optimistic company. For most of our existence, we focused on all the good that connecting people can bring. And as Facebook has grown, people everywhere have gotten a powerful new tool for staying connected to the people they care about most, for making their voices heard, and for building community and businesses.

Just recently, we have seen the Me Too movement and the March for Our Lives organized at least part on Facebook. After Hurricane Harvey, people came together and raised more than \$20 million for relief, and there are more than 70 million small businesses around the world that use our tools to grow and create jobs.

But it is clear now that we didn't do enough to prevent these tools from being used for harm as well. And that goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake. It was my mistake, and I am sorry.

I started Facebook. I run it. And at the end of the day, I am responsible for what happens here. So now we have to go through every part of our relationship with people to make sure that we are taking a broad enough view of our responsibility.

It is not enough to just connect people; we have to make sure that those connections are positive. It is not enough to just give people a voice; we need to make sure that that voice isn't used to harm other people or spread misinformation.

And it is not enough to just give people control of their information; we need to make sure that the developers that they share it with protect their information too. Across the board, we have a responsibility to not just give people tools but to make sure that those tools are used for good.

It is going to take some time to work through all the changes we need to make, but I am committed to getting this right. And that includes the basic responsibility of protecting people's information, which we failed to do with Cambridge Analytica.

So here are a few key things that we are doing to address this situation and make sure that this doesn't happen again. First, we are getting to the bottom of exactly what Cambridge Analytica did and telling everyone who may have been affected.

What we know now is that Cambridge Analytica improperly obtained some information about millions of Facebook members by

buying it from an app developer that people had shared it with. This information was generally information that people share publicly on their profile pages, like their name and profile picture and the list of pages that they follow.

When we first contacted Cambridge Analytica, they told us that they had deleted the data. And then, about a month ago, we heard a new report that suggested that this was not true. So now we are working with governments in the U.S., the U.K., and around the world to do a full audit of what they have done and to make sure that they get rid of any data that they still have.

Second, to make sure that no other app developers are out there misusing data, we are now investigating every single app that had access to a large amount of people's information on Facebook in the past. And if we find someone that improperly used data, we are going to ban them from our platform and tell everyone affected.

Third, to prevent this from ever happening again, we are making sure developers can't access as much information going forward. The good news here is that we made some big changes to our platform in 2014 that would prevent this specific instance with Cambridge Analytica from happening again today.

There is more to do, and you can find more of the details of the other steps we are taking in the written statement I provided.

My top priority has always been our social mission of connecting people, building community, and bringing the world closer together. Advertisers and developers will never take priority over that for as long as I am running Facebook.

I started Facebook when I was in college. We have come a long way since then. We now serve more than 2 billion people around the world, and every day people use our services to stay connected with the people that matter to them most.

I believe deeply in what we are doing, and I know that, when we address these challenges, we will look back and view helping people connect and giving more people a voice as a positive force in the world.

I realize the issues we are talking about today aren't just issues for Facebook and our community; they are challenges for all of us as Americans. Thank you for having me here today, and I am ready to take your questions.

[The prepared statement of Mr. Zuckerberg follows:]

**HEARING BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES  
COMMITTEE ON ENERGY AND COMMERCE**

April 11, 2018

Testimony of Mark Zuckerberg  
Chairman and Chief Executive Officer, Facebook

**I. INTRODUCTION**

Chairman Walden, Ranking Member Pallone, and Members of the Committee,

We face a number of important issues around privacy, safety, and democracy, and you will rightfully have some hard questions for me to answer. Before I talk about the steps we're taking to address them, I want to talk about how we got here.

Facebook is an idealistic and optimistic company. For most of our existence, we focused on all the good that connecting people can bring. As Facebook has grown, people everywhere have gotten a powerful new tool to stay connected to the people they love, make their voices heard, and build communities and businesses. Just recently, we've seen the #metoo movement and the March for Our Lives, organized, at least in part, on Facebook. After Hurricane Harvey, people raised more than \$20 million for relief. And more than 70 million small businesses now use Facebook to grow and create jobs.

But it's clear now that we didn't do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake. It was my mistake, and I'm sorry. I started Facebook, I run it, and I'm responsible for what happens here.

So now we have to go through every part of our relationship with people and make sure we're taking a broad enough view of our responsibility.

It's not enough to just connect people, we have to make sure those connections are positive. It's not enough to just give people a voice, we have to make sure people aren't using it to hurt people or spread misinformation. It's not enough to give people control of their information, we have to make sure developers they've given it to are protecting it too. Across the board, we have a responsibility to not just build tools, but to make sure those tools are used for good.

It will take some time to work through all of the changes we need to make, but I'm committed to getting it right.

That includes improving the way we protect people's information and safeguard elections around the world. Here are a few key things we're doing:

## II. CAMBRIDGE ANALYTICA

Over the past few weeks, we've been working to understand exactly what happened with Cambridge Analytica and taking steps to make sure this doesn't happen again. We took important actions to prevent this from happening again today four years ago, but we also made mistakes, there's more to do, and we need to step up and do it.

### A. What Happened

In 2007, we launched the Facebook Platform with the vision that more apps should be social. Your calendar should be able to show your friends' birthdays, your maps should show where your friends live, and your address book should show their pictures. To do this, we enabled people to log into apps and share who their friends were and some information about them.

In 2013, a Cambridge University researcher named Aleksandr Kogan created a personality quiz app. It was installed by around 300,000 people who agreed to share some of their Facebook information as well as some information from their friends whose privacy settings allowed it. Given the way our platform worked at the time this meant Kogan was able to access some information about tens of millions of their friends.

In 2014, to prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the Facebook information apps could access. Most importantly, apps like Kogan's could no longer ask for information about a person's friends unless their friends had also authorized the app. We also required developers to get approval from Facebook before they could request any data beyond a user's public profile, friend list, and email address. These actions would prevent any app like Kogan's from being able to access as much Facebook data today.

In 2015, we learned from journalists at *The Guardian* that Kogan had shared data from his app with Cambridge Analytica. It is against our policies for developers to share data without people's consent, so we immediately banned Kogan's app from our platform, and demanded that Kogan and other entities he gave the data to, including Cambridge Analytica, formally certify that they had deleted all improperly acquired data — which they ultimately did.

Last month, we learned from *The Guardian*, *The New York Times* and Channel 4 that Cambridge Analytica may not have deleted the data as they had certified. We immediately banned them from using any of our services. Cambridge Analytica claims they have already deleted the data and has agreed to a forensic audit by a firm we hired to investigate this. We're also working with the U.K. Information Commissioner's Office, which has jurisdiction over Cambridge Analytica, as it completes its investigation into what happened.

### B. What We Are Doing

We have a responsibility to make sure what happened with Kogan and Cambridge Analytica doesn't happen again. Here are some of the steps we're taking:

- *Safeguarding our platform.* We need to make sure that developers like Kogan who got access to a lot of information in the past can't get access to as much information going forward.
  - We made some big changes to the Facebook platform in 2014 to dramatically restrict the amount of data that developers can access and to proactively review the apps on our platform. This makes it so a developer today can't do what Kogan did years ago.
  - But there's more we can do here to limit the information developers can access and put more safeguards in place to prevent abuse.
    - We're removing developers' access to your data if you haven't used their app in three months.
    - We're reducing the data you give an app when you approve it to only your name, profile photo, and email address. That's a lot less than apps can get on any other major app platform.
    - We're requiring developers to not only get approval but also to sign a contract that imposes strict requirements in order to ask anyone for access to their posts or other private data.
    - We're restricting more APIs like groups and events. You should be able to sign into apps and share your public information easily, but anything that might also share other people's information — like other posts in groups you're in or other people going to events you're going to — will be much more restricted.
    - Two weeks ago, we found out that a feature that lets you look someone up by their phone number and email was abused. This feature is useful in cases where people have the same name, but it was abused to link people's public Facebook information to a phone number they already had. When we found out about the abuse, we shut this feature down.
- *Investigating other apps.* We're in the process of investigating every app that had access to a large amount of information before we locked down our platform in 2014. If we detect suspicious activity, we'll do a full forensic audit. And if we find that someone is improperly using data, we'll ban them and tell everyone affected.
- *Building better controls.* Finally, we're making it easier to understand which apps you've allowed to access your data. This week we started showing everyone a list of the apps you've used and an easy way to revoke their permissions to your data. You can already do this in your privacy settings, but we're going to put it at the top of News Feed to make sure everyone sees it. And we also told everyone whose Facebook information may have been shared with Cambridge Analytica.



Beyond the steps we had already taken in 2014, I believe these are the next steps we must take to continue to secure our platform.

### **III. RUSSIAN ELECTION INTERFERENCE**

Facebook's mission is about giving people a voice and bringing people closer together. Those are deeply democratic values and we're proud of them. I don't want anyone to use our tools to undermine democracy. That's not what we stand for.

We were too slow to spot and respond to Russian interference, and we're working hard to get better. Our sophistication in handling these threats is growing and improving quickly. We will continue working with the government to understand the full extent of Russian interference, and we will do our part not only to ensure the integrity of free and fair elections around the world, but also to give everyone a voice and to be a force for good in democracy everywhere.

#### **A. What Happened**

Elections have always been especially sensitive times for our security team, and the 2016 U.S. presidential election was no exception.

Our security team has been aware of traditional Russian cyber threats — like hacking and malware — for years. Leading up to Election Day in November 2016, we detected and dealt with several threats with ties to Russia. This included activity by a group called APT28, that the U.S. government has publicly linked to Russian military intelligence services.

But while our primary focus was on traditional threats, we also saw some new behavior in the summer of 2016 when APT28-related accounts, under the banner of DC Leaks, created fake personas that were used to seed stolen information to journalists. We shut these accounts down for violating our policies.

After the election, we continued to investigate and learn more about these new threats. What we found was that bad actors had used coordinated networks of fake accounts to interfere in the election: promoting or attacking specific candidates and causes, creating distrust in political institutions, or simply spreading confusion. Some of these bad actors also used our ads tools.

We also learned about a disinformation campaign run by the Internet Research Agency (IRA) — a Russian agency that has repeatedly acted deceptively and tried to manipulate people in the US, Europe, and Russia. We found about 470 accounts and pages linked to the IRA, which generated around 80,000 Facebook posts over about a two-year period.

Our best estimate is that approximately 126 million people may have been served content from a Facebook Page associated with the IRA at some point during that period. On Instagram, where our data on reach is not as complete, we found about 120,000 pieces of content, and estimate that an additional 20 million people were likely served it.

Over the same period, the IRA also spent approximately \$100,000 on more than 3,000 ads on

Facebook and Instagram, which were seen by an estimated 11 million people in the United States. We shut down these IRA accounts in August 2017.

#### **B. What We Are Doing**

There's no question that we should have spotted Russian interference earlier, and we're working hard to make sure it doesn't happen again. Our actions include:

- *Building new technology to prevent abuse.* Since 2016, we have improved our techniques to prevent nation states from interfering in foreign elections, and we've built more advanced AI tools to remove fake accounts more generally. There have been a number of important elections since then where these new tools have been successfully deployed. For example:
  - In France, leading up to the presidential election in 2017, we found and took down 30,000 fake accounts.
  - In Germany, before the 2017 elections, we worked directly with the election commission to learn from them about the threats they saw and to share information.
  - In the U.S. Senate Alabama special election last year, we deployed new AI tools that proactively detected and removed fake accounts from Macedonia trying to spread misinformation.
  - We have disabled thousands of accounts tied to organized, financially motivated fake news spammers. These investigations have been used to improve our automated systems that find fake accounts.
  - Last week, we took down more than 270 additional pages and accounts operated by the IRA and used to target people in Russia and Russian speakers in countries like Azerbaijan, Uzbekistan and Ukraine. Some of the pages we removed belong to Russian news organizations that we determined were controlled by the IRA.
- *Significantly increasing our investment in security.* We now have about 15,000 people working on security and content review. We'll have more than 20,000 by the end of this year.
  - I've directed our teams to invest so much in security — on top of the other investments we're making — that it will significantly impact our profitability going forward. But I want to be clear about what our priority is: protecting our community is more important than maximizing our profits.
- *Strengthening our advertising policies.* We know some Members of Congress are exploring ways to increase transparency around political or issue advertising, and we're happy to keep working with Congress on that. But we aren't waiting for legislation to act.

- From now on, every advertiser who wants to run political or issue ads will need to be authorized. To get authorized, advertisers will need to confirm their identity and location. Any advertiser who doesn't pass will be prohibited from running political or issue ads. We will also label them and advertisers will have to show you who paid for them. We're starting this in the U.S. and expanding to the rest of the world in the coming months.
- For even greater political ads transparency, we have also built a tool that lets anyone see all of the ads a page is running. We're testing this in Canada now and we'll launch it globally this summer. We're also creating a searchable archive of past political ads.
- We will also require people who manage large pages to be verified as well. This will make it much harder for people to run pages using fake accounts, or to grow virally and spread misinformation or divisive content that way.
- In order to require verification for all of these pages and advertisers, we will hire thousands of more people. We're committed to getting this done in time for the critical months before the 2018 elections in the U.S. as well as elections in Mexico, Brazil, India, Pakistan and elsewhere in the next year.
- These steps by themselves won't stop all people trying to game the system. But they will make it a lot harder for anyone to do what the Russians did during the 2016 election and use fake accounts and pages to run ads. Election interference is a problem that's bigger than any one platform, and that's why we support the Honest Ads Act. This will help raise the bar for all political advertising online.
- *Sharing information.* We've been working with other technology companies to share information about threats, and we're also cooperating with the U.S. and foreign governments on election integrity.

At the same time, it's also important not to lose sight of the more straightforward and larger ways Facebook plays a role in elections.

In 2016, people had billions of interactions and open discussions on Facebook that may never have happened offline. Candidates had direct channels to communicate with tens of millions of citizens. Campaigns spent tens of millions of dollars organizing and advertising online to get their messages out further. And we organized "get out the vote" efforts that helped more than 2 million people register to vote who might not have voted otherwise.

Security — including around elections — isn't a problem you ever fully solve. Organizations like the IRA are sophisticated adversaries who are constantly evolving, but we'll keep improving our techniques to stay ahead. And we'll also keep building tools to help more people make their voices heard in the democratic process.

**IV. CONCLUSION**

My top priority has always been our social mission of connecting people, building community and bringing the world closer together. Advertisers and developers will never take priority over that as long as I'm running Facebook.

I started Facebook when I was in college. We've come a long way since then. We now serve more than 2 billion people around the world, and every day, people use our services to stay connected with the people that matter to them most. I believe deeply in what we're doing. And when we address these challenges, I know we'll look back and view helping people connect and giving more people a voice as a positive force in the world.

I realize the issues we're talking about today aren't just issues for Facebook and our community — they're challenges for all of us as Americans. Thank you for having me here today, and I'm ready to take your questions.

Mr. WALDEN. Thank you, Mr. Zuckerberg.

I will start out. When we go into the questioning phase, we go back and forth, as we always do. Remember, it is 4 minutes today so we can get to everyone.

Mr. Zuckerberg, you described Facebook as a company that connects people and as a company that is idealistic and optimistic. I have a few questions about what other types of companies Facebook may be.

Facebook has created its own video series starring Tom Brady that ran for six episodes and has over 50 million views. That is twice the number of the viewers that watched the Oscars last month. Also, Facebook has obtained exclusive broadcasting rights for 25 major league baseball games this season. Is Facebook a media company?

Mr. ZUCKERBERG. Thank you, Mr. Chairman.

I consider us to be a technology company because the primary thing that we do is have engineers who write code and build products and services for other people. There are certainly other things that we do too.

We do pay to help produce content. We build enterprise software although I don't consider us an enterprise software company. We build planes to help connect people, and I don't consider ourselves to be an aerospace company.

But, overall, when people ask us if we are a media company, what I hear is, do we have a responsibility for the content that people share on Facebook? And I believe the answer to that question is yes.

Mr. WALDEN. All right. Let me ask the next one. You can send money to friends on Facebook Messenger using a debit card or a PayPal account to, quote, "split meals, pay rent, and more," closed quote. People can also send money via Venmo or their bank app. Is Facebook a financial institution?

Mr. ZUCKERBERG. Mr. Chairman, I do not consider ourselves to be a financial institution although you are right that we do provide tools for people to send money.

Mr. WALDEN. So you have mentioned several times that you started Facebook in your dorm room, 2004. 15 years, 2 billion users and several, unfortunately, breaches of trust later, is Facebook today the same kind of company you started with a Harvard.edu email address?

Mr. ZUCKERBERG. Well, Mr. Chairman, I think we have evolved quite a bit as a company. When I started it, I certainly didn't think that we would be the ones building this broad of a community around the world. I thought someone would do it. I didn't think it was going to be us. So we have definitely grown.

Mr. WALDEN. And you have recently said that you and Facebook have not done a good job of explaining what Facebook does. And so, back in 2012 and 2013, when a lot of this scraping of user and friend data was happening, did it ever cross your mind that you should be communicating more clearly with users about how Facebook is monetizing their data?

I understand that Facebook does not sell user data, per se, in the traditional sense. But it is also just as true that Facebook's user

data is probably the most valuable thing about Facebook. In fact, it may be the only truly valuable thing about Facebook.

Why wasn't explaining what Facebook does with users' data higher priority for you as a cofounder and now as CEO?

Mr. ZUCKERBERG. Mr. Chairman, you are right that we don't sell any data, and I would say that we do try to explain what we do as time goes on. It is a broad system. You know, every day, about 100 billion times a day, people come to one of our products, whether it is Facebook or Messenger or Instagram or WhatsApp, to put in a piece of content, whether it is a photo that they want to share or a message they want to send someone, and every time there is a control right there about who you want to share it with.

Do you want to share it publicly to broadcast it out to everyone? Do you want to share it with your friends, a specific group of people? Do you want to message it to just one person or a couple of people? That is the most important thing that we do, and I think that in the product that is quite clear.

I do think that we can do a better job of explaining how advertising works. There is a common misperception, as you say, that is just reported—often keeps on being reported—that for some reason we sell data.

I can't be clearer on this topic: We don't sell data. That is now how advertising works. And I do think we could probably be doing a clearer job explaining that, given the misperceptions that are out there.

Mr. WALDEN. Given the situation, can you manage the issues that are before you, or does the Congress need to intercede? I am going to leave that because I am over my time. That and I want to flag an issue that Vietnam Veterans of America have raised too, and we will get back with your staff on that, about some fake pages that are up.

But I want to stay on schedule. So, with that, I will yield to Mr. Pallone for 4 minutes.

Mr. PALLONE. Thank you.

Mr. Zuckerberg, you talked about how positive and optimistic you are, and I am—I guess, I am sorry, because I am not. I don't have much faith in corporate America, and I certainly don't have much faith in their GOP allies here in Congress.

I really look at everything that this committee does, or most of what this committee does, in terms of the right to know. In other words, I always fear that people, you know, that go onto Facebook, they don't necessarily know what is happening or what is going on with their data.

And so, to the extent that we could pass legislation—which I think we need, and you said that we probably should have some legislation—I want that legislation to give people the right to know, to empower them, to, you know, provide more transparency, I guess, is the best way to put it.

So I am looking at everything through that sort of lens. So just let me ask you three quick questions, and I am going to ask you to answer yes or no because of the time. Yes or no, is Facebook limiting the amount or type of data Facebook itself collects or uses?

Mr. ZUCKERBERG. Congressman, yes. We limit a lot of the data that we collect and use.

Mr. PALLONE. But, see, I don't see that in the announcements you have made. Like, you have made all these announcements the last few days about the changes you are going to make, and I don't really see how those announcements or changes limit the amount or type of data that Facebook collects or uses in an effective way.

But let me go to the second one. Again, this is my concern that users currently may not know or take affirmative action to protect their own privacy. Yes or no, is Facebook changing any user default settings to be more privacy protective?

Mr. ZUCKERBERG. Congressman, yes. In response to these issues, we have changed a lot of the way that our platform works so they way developers can't get access to as much information.

Mr. PALLONE. But, see, again, I don't see that in the changes that you have proposed. I don't really see any way that these users' default settings—or you are changing these user default settings in a way that is going to be more privacy protection—protected.

But let me go to the third one. Yes or no, will you commit to changing all the user default settings to minimize to the greatest extent possible the collection in user—in use of users' data? Can you make that commitment?

Mr. ZUCKERBERG. Congressman, we try to collect and give people the ability to share—

Mr. PALLONE. But I would like you to answer yes or no, if you could. Will you make the commitment to change all the user—to changing all the user default settings to minimize to the greatest extent possible the collection and use of users' data? I don't think that is hard for you to say yes to, unless I am missing something.

Mr. ZUCKERBERG. Congressman, this is a complex issue that I think deserves more than a one-word answer.

Mr. PALLONE. Well, again, that is disappointing to me, because I think you should make that commitment. And maybe what we could do is follow up with you on this, if possible, if that is OK. We can do that follow up?

Mr. ZUCKERBERG. Yes.

Mr. PALLONE. All right. Now, you said yesterday that each of us owns the content that we put on Facebook and that Facebook gives some control to consumers over their content, but we know about the problems with Cambridge Analytica.

I know you changed your rules in 2014 and again this week, but you still allow third parties to have access to personal data. How can consumers have control over their data when Facebook doesn't have control over the data itself? That is my concern. Last question.

Mr. ZUCKERBERG. Congressman, what we allow with our developer platform is for people to choose to sign into other apps and bring their data with them. That is something that a lot of people want to be able to do.

The reason why we built the developer platform in the first place was because we thought it would be great if more experiences that people had could be more social. So, if you could have a calendar that showed your friends' birthdays, if you could have an address book that had pictures of your friends in it, if you could have a map that showed your friends' addresses on it.

In order to do that, you need to be able to sign into an app, bring some of your data and some of your friends' data, and that is what we built. Now, since then, we have recognized that that can be used for abuse too, so we have limited it so now people can only bring their data when they go to an app.

But that is something that a lot of people do on a day-to-day basis is sign into apps and websites with Facebook, and that is something that we are going—

Mr. WALDEN. We have to move onto our next question.

Mr. PALLONE. Yes, I know. I still think that there is not enough—people aren't empowered enough to really make those decisions in a positive way.

Mr. WALDEN. The Chair now recognizes former chairman of the committee Mr. Barton of Texas for 4 minutes.

Mr. BARTON. Well, thank you.

And thank you, Mr. Zuckerberg, for being here. People need to know that you are here voluntarily. You are not here because you have been subpoenaed, so we appreciate that.

Sitting behind you, I have a gentleman that used to be counsel for the committee, Mr. Jim Barnett. And if he is affiliated with Facebook, you have got a good one. If he is not, he has just got a great seat. I don't know what it is.

I am going to read you a question that I was asked—I got this through Facebook. And I have got dozens like this. So my first question: "Please ask Mr. Zuckerberg, why is Facebook censoring conservative bloggers, such as Diamond and Silk? Facebook called them unsafe to the community. That is ludicrous. They hold conservative views. That isn't unsafe." What is your response to that?

Mr. ZUCKERBERG. Congressman, in that specific case, our team made an enforcement error, and we have already gotten in touch with them to reverse it.

Mr. BARTON. Well, Facebook does tremendous good. When I met you in my office 8 years ago—you don't remember that—but I have got a picture of you when you had curly hair, and Facebook had 500 million users. Now it has got over 2 billion. That is a success story in anybody's book.

It is such an integral part of certainly young Americans' lives that you need to work with Congress and the community to ensure that it is a neutral, safe, and, to the largest extent possible, private platform. Do you agree with that?

Mr. ZUCKERBERG. Congressman, I do agree that we should work to give people the fullest free expression that is possible. That is—when I talk about giving people a voice, that is what I care about.

Mr. BARTON. OK. Let's talk about children. Children can get a Facebook account of their own, I believe, starting at age 13. Is that not correct?

Mr. ZUCKERBERG. Congressman, that is correct.

Mr. BARTON. OK. Is there any reason that we couldn't have just a no-data-sharing policy period until you are 18? Just, if you are a child with your own Facebook account, until you reach the age of 18, you know, it is, you know, you can't share anything? It is their data, their—it doesn't go anywhere. Nobody gets to scrape it. Nobody gets to access it. It is absolutely totally private for children. What is wrong with that?



Mr. ZUCKERBERG. Congressman, we have a number of measures in place to protect minors specifically. We make it so that adults can't contact minors who they aren't already friends with. We make it so that certain content that may be inappropriate for minors we don't show.

The reality that we see is that teens often do want to share their opinions publicly, and that is a service that—

Mr. BARTON. Then we let them opt in to do that?

Mr. ZUCKERBERG. Yes, we do.

Mr. BARTON. But don't—you know, unless they specifically allow it, then don't allow it. That is my point.

Mr. ZUCKERBERG. Congressman, every time that someone chooses to share something on Facebook, you go to the app, right there, it says, "Who do you want to share with?" When you sign up for a Facebook account, it starts off sharing with just your friends. If you want to share it publicly, you have to specifically go and change that setting to be sharing publicly. And every time—

Mr. BARTON. I am about out of time. I actually use Facebook. And, you know, I know if you take the time, you can go to your privacy and click on that and you can go to your settings and click on that. You can pretty well set up your Facebook account to be almost totally private, but you have to really work at it.

And my time has expired. Hopefully we can do some questions in writing as a followup.

Mr. WALDEN. Absolutely.

Mr. BARTON. Thank you, Mr. Chairman.

Mr. WALDEN. The Chair now recognizes the gentleman from Illinois, Mr. Rush, for 4 minutes for questions.

Mr. RUSH. Thank you, Mr. Chairman.

Mr. Zuckerberg, welcome.

In the 1960s, our Government, acting through the FBI and local police, maliciously tricked individuals and organizations into participating in something called COINTELPRO, which was a counter-intelligence program where they tracked and shared information about civil rights activists, their political, social, civic, even religious affiliations, and I personally was a victim of COINTELPRO.

Your organization, your methodology, in my opinion, is similar. You are truncating the basic rights of the American promise of life, liberty, and the pursuit of happiness by the wholesale invasion and manipulation of their right to privacy.

Mr. Zuckerberg, what is the difference between Facebook's methodology and the methodology of the American political pariah J. Edgar Hoover?

Mr. ZUCKERBERG. Congressman, this is an important question because I think people often ask what the difference is between surveillance and what we do. And I think that the difference is extremely clear, which is that, on Facebook, you have control over your information. The content that you share, you put there. You can take it down at any time.

The information that we collect you can choose to have us not collect. You can delete any of it. And, of course, you can leave Facebook if you want. I know of no surveillance organization that gives people the option to delete the data that they have or even know what they are collecting.

Mr. RUSH. Mr. Zuckerberg, you should be commended that Facebook has grown so big, so fast. It is no longer the company that you started in your dorm room. Instead, it is one of the great American success stories.

That much influence comes with enormous social responsibility on which you have failed to act and to protect and to consider. Shouldn't Facebook, by default, protect users' information? Why is the onus on the user to opt in to privacy and security settings?

Mr. ZUCKERBERG. Congressman, as I said, every time that a person chooses to share something on Facebook, they are proactively going to the service and choosing that they want to share a photo, write a message to someone. And every time, there is a control right there, not buried in settings somewhere, but right there when they are posting about who they want to share it with.

Mr. RUSH. Mr. Zuckerberg, I only have a few more seconds. In November 2017, ProPublica reported that Facebook was still allowing housing advertisements to systemically exclude advertisements to specific racial groups, an explicitly prohibited practice. This is just one example where Facebook has allowed race to improperly play a role.

What has Facebook done, and what are you going to do to ensure that your targeted advertisements and other components of your platform are in compliance with Federal laws, such as the Civil Rights Act of 1968?

Mr. ZUCKERBERG. Congressman, since we learned about that, we removed the option for advertisers to exclude ethnic groups from targeting.

Mr. RUSH. When did you do that?

Mr. WALDEN. The gentleman's time has expired. We need to go now to the gentleman from Michigan, Mr. Upton, for 4 minutes.

Mr. UPTON. Thank you, Mr. Chairman.

And welcome to the committee.

A number of times in the last day or two you have indicated that, in fact, you are now open to some type of regulation. And we know, of course, that you are the dominant social media platform without any true competitor, in all frankness, and you have hundreds, if not thousands, of folks that are—would be required to help navigate any type of regulatory environment.

Some would argue that a more regulatory environment might ultimately stifle new platforms and innovators some might describe as desperately needed competition, i.e., regulatory complexity helps protect those folks like you. It could create a harmful barrier to entry for some startups, particularly ones that might want to compete with you.

So should we policymakers up here be more focused on the needs of startups over large incumbents, and what kind of policy regulation—regulatory environment would you want instead of managing maybe a Fortune 500 company if you were launching a startup to take on the big guy?

Mr. ZUCKERBERG. Congressman, thank you. And let me say a couple of things on this. First, to your point about competition, the average American uses about eight different apps to communicate and stay connected to people. So there is a lot of competition that

we feel every day, and that is an important force that we definitely feel in running the company.

Second, on your point about regulation, the internet is growing in importance around the world in peoples' lives, and I think that it is inevitable that there will need to be some regulation. So my position is not that there should be no regulation, but I also think that you have to be careful about what regulation you put in place for a lot of the reasons that you are saying.

I think a lot of times regulation, by definition, puts in place rules that a company that is larger, that has resources like ours, can easily comply with but that might be more difficult for a smaller start-up to comply with.

So I think that these are all things that need to be thought through very carefully when thinking through what rules we want to put in place.

Mr. UPTON. To follow up on a question that Mr. Barton asked about Silk and Diamond, I don't know whether you know about this particular case. I have a former State rep who is running for State senate. He is the former Michigan lottery commissioner, so he is a guy of fairly good political prominence.

He announced for State senate just in the last week, and he had what I thought was a rather positive announcement, and I will read to you precisely what it was: "I am proud to announce my candidacy for State Senate. Lansing needs conservative west Michigan values. And as our next State senator, I will work to strengthen our economy, limit Government, lower our auto insurance rates, balance the budget, stop sanctuary cities, pay down Government debt, be a pro-life, pro-Second Amendment lawmaker," end.

It was rejected, and the response from you all was: It wasn't approved because it doesn't follow our advertising policies; we don't allow ads that contain shocking, disrespectful, or sensational content, including ads that depict violence or threats of violence.

I am not sure where the threat was based on what he tried to post.

Mr. ZUCKERBERG. Congressman, I am not sure either. I am not familiar with that specific case. It is quite possible that we made a mistake, and we will follow up afterwards on that.

Mr. UPTON. OK.

Mr. ZUCKERBERG. Overall, we have—by the end of this year, we will have about 20,000 people at the company who work on security and content review-related issues, but there is a lot of content flowing through the systems and a lot of reports, and unfortunately, we don't always get these things right when people report it to us.

Mr. UPTON. Thank you.

Mr. WALDEN. The gentleman's time has expired.

The Chair recognizes the gentlelady from California, Ms. Eshoo, for 4 minutes.

Ms. ESHOO. Thank you, Mr. Chairman.

Good morning, Mr. Zuckerberg.

First, I believe that our democratic institutions are undergoing a stress test in our country. And I believe that American companies owe something to America. I think the damage done to our democracy relative to Facebook and its platform being weaponized are incalculable.

Enabling the cynical manipulation of American citizens for the purpose of influencing an election is deeply offensive, and it is very dangerous. Putting our private information on offer without concern for possible misuses, I think, is simply irresponsible.

I invited my constituents, going into the weekend, to participate in this hearing today by submitting what they want to ask you, and so my questions are theirs.

And, Mr. Chairman, I would like unanimous consent to place all of their questions in the record.

Mr. WALDEN. Without objection.

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

Ms. ESHOO. So these are a series of just yes-or-no questions. Do you think you have a moral responsibility to run a platform that protects our democracy, yes or no?

Mr. ZUCKERBERG. Congresswoman, yes.

Ms. ESHOO. Have users of Facebook who were caught up in the Cambridge Analytica debacle been notified?

Mr. ZUCKERBERG. Yes, we were starting to notify people this week. We started Monday, I believe.

Ms. ESHOO. Will Facebook offer to all of its users a blanket opt-in to share their privacy data with any third-party users?

Mr. ZUCKERBERG. Congresswoman, yes, that is how our platform works. You have to opt in to sign into any app before you use it.

Ms. ESHOO. Well, let me just add that it is a minefield in order to do that. And you have to make it transparent, clear, in pedestrian language just once: "This is what we will do with your data. Do you want this to happen or not?" So I think that this is being blurred. I think you know what I mean by it.

Are you aware of other third-party information mishandlings that have not been disclosed?

Mr. ZUCKERBERG. Congresswoman, no, although we are currently going through the process of investigating every single app—

Ms. ESHOO. So you are not sure?

Mr. ZUCKERBERG [continuing]. That had access to a large amount of data.

Ms. ESHOO. What does that mean?

Mr. ZUCKERBERG. It means that we are going to look into every app that had a large amount of access to data in the past before we lock down the platform.

Ms. ESHOO. You are not aware?

Mr. ZUCKERBERG. I imagine that, because there are tens of thousands of apps, we will find some that have suspicious activity, and when we find them—

Ms. ESHOO. All right. I only have 4 minutes.

Was your data included in the data sold to the malicious third parties, your personal data?

Mr. ZUCKERBERG. Yes.

Ms. ESHOO. It was? Are you willing to change your business model in the interest of protecting individual privacy?

Mr. ZUCKERBERG. Congresswoman, we have made and are continuing to make changes to reduce the amount of data that—

Ms. ESHOO. No. Are you willing to change your business model in the interest of protecting individual privacy?

Mr. ZUCKERBERG. Congresswoman, I am not sure what that means.

Ms. ESHOO. Well, I will follow up with you on it.

When did Facebook learn that Cambridge Analytica's research project was actually for targeted psychographic political campaign work?

Mr. ZUCKERBERG. Congresswoman, it might be useful to clarify what actually happened here. A developer who is a researcher—

Ms. ESHOO. Well, no. I don't have time for a long answer, though. When did Facebook learn that? And when you learned it, did you contact their CEO immediately, and if not, why not?

Mr. ZUCKERBERG. Congresswoman, yes. When we learned in 2015 that a Cambridge University researcher associated with the academic institution that built an app that people chose to share their data with—

Ms. ESHOO. We know what happened with them, but I am asking you.

Mr. ZUCKERBERG. Yes, I am answering your question.

Ms. ESHOO. Right.

Mr. ZUCKERBERG. When we learned about that, we immediately—

Ms. ESHOO. So, in 2015, you learned about it?

Mr. ZUCKERBERG. Yes.

Ms. ESHOO. And you spoke to their CEO immediately?

Mr. ZUCKERBERG. We shut down the app. We demanded—

Ms. ESHOO. Did you speak to their CEO immediately?

Mr. ZUCKERBERG. We got in touch with them, and we asked them to—we demanded that they delete any of the data that they had, and their chief data officer told us that they had.

Mr. WALDEN. The gentlelady's time has expired.

Ms. ESHOO. Thank you.

Mr. WALDEN. The Chair now recognizes the gentleman from Illinois, Mr. Shimkus, for 4 minutes.

Mr. SHIMKUS. Thank you, Mr. Chairman.

Thank you for being here, Mr. Zuckerberg.

Two things: First of all, I want to thank Facebook. You streamlined our congressional baseball game last year. We have got the managers here. And I was told that, because of that, we raised an additional \$100,000 for DC literacy and feeding kids and stuff, so that is—

The other thing is, I usually put my stuff up on the TV. I don't want to do it very much because it is my dad, and he would be mad if he went international like you are. And he has been on Facebook for a long time. He is 88. It has been good for connecting with kids and grandkids.

I just got my mother involved on an iPad and—because she can't handle a keyboard. And so—and I did this last week. So, in the swirl of activity, I still think there is a positive benefit for my parents to be engaged on this platform. So—but there are issues that are being raised today, and so I am going to go into a couple of those.

Facebook made, developed access to user and friend data back—and your main update was in 2014. So the question is, what triggered that update?

Mr. ZUCKERBERG. Congressman, this is an important question to clarify. So, in 2007, we launched the platform in order to make it so that people could sign into other apps, bring some of their information and some of their friends' information to have social experiences.

This created a lot of innovative experiences, new games, companies like Zynga. There were companies that you are familiar with like Netflix and Spotify had integrations with this that allowed social experiences in their apps. But, unfortunately, there were also a number of apps that used this for abuse, to collect people's data.

Mr. SHIMKUS. So, if I could interrupt, you identified that there was possibly social scraping going on?

Mr. ZUCKERBERG. Yes, there was abuse. And that is why, in 2014, we took the step of fundamentally changing how the platform works. So now, when you sign into an app, you can bring your information, and if a friend has also signed into the app, then the app can know that you are friends so you can have a social experience in that app. But when you sign into an app, it now no longer brings information from other people.

Mr. SHIMKUS. Yes. Let me go to your announcement of audits. Who is going to conduct an audit when we are talking about are there other Cambridge Analyticas out there?

Mr. ZUCKERBERG. Yes, Congressman. Good question.

So we are going to start by doing an investigation internally of every single app that had access to a large amount of information before we lock down the platform. If we detect any suspicious activity at all, we are working with third-party auditors. I imagine there will have to be a number of them because there are a lot of apps, and they will conduct the audit for us.

Mr. SHIMKUS. Yes. I think we would hope that you would bring in a third party to help us—

Mr. ZUCKERBERG. Yes.

Mr. SHIMKUS [continuing]. Clarify and have more confidence.

The last question I have is, in yesterday's hearing, you talked a little about Facebook tracking and different scenarios, including logged-off users. Can you please clarify as to how that works and how does tracking work across different devices?

Mr. ZUCKERBERG. Yes, Congressman. Thank you for giving me the opportunity to clarify that.

So one of the questions is, what information do we track and why about people who are not signed into Facebook? We track certain information for security reasons and for ads reasons. For security, it is to make sure that people who are not signed into Facebook can't scrape people's public information.

You can—even when you are not signed in, you can look up the information that people have chosen to make public on their page because they wanted to share it with everyone, so there is no reason why you should have to be logged in.

But, nonetheless, we don't want someone to be able to go through and download every single public piece of information. Even if someone chose to make it public, that doesn't mean that it is good to allow someone to aggregate it. So, even if someone isn't logged in, we track certain information, like how many pages they are accessing, as a security measure.

The second thing that we do is we provide an ad network that third-party websites and apps can run in order to help them make money. And those ads, similar to what Google does and what the rest of the industry does, it is not limited to people who are just on Facebook. So, for the purposes of that, we may also collect information to make it so that those ads are more relevant and work better on those websites.

There is a control that for that second class of information or an ad targeting anyone can turn off, has complete control over it. For obvious reasons, we do not allow people to turn off the measurement that we do around security.

Mr. WALDEN. The gentleman's time has expired.

We now turn to the gentleman from New York, Mr. Engel, for 4 minutes.

Mr. ENGEL. Thank you, Mr. Chairman.

Mr. Zuckerberg, you have roots in my district, the 16th Congressional District of New York. I know that you attended Ardsley High School and grew up in Westchester County. As you know, Westchester has a lot to offer, and I hope that you might commit to returning to Westchester County perhaps to do a forum on this and some other things. I hope you would consider that. We will be in touch with you. But I know that Ardsley High School is very proud of you.

You mentioned yesterday that Facebook was deceived by Aleksandr Kogan when he sold the user information to Cambridge Analytica. Does Facebook therefore plan to sue Aleksandr Kogan, Cambridge University, or Cambridge Analytica perhaps for unauthorized access to computer networks, exceeding access to computer networks, or breach of contract, and why or why not?

Mr. ZUCKERBERG. Congressman, it is something that we are looking into. We already took action by banning him from the platform, and we are going to be doing a full audit to make sure that he gets rid of all the data that he has as well.

To your point about Cambridge University, what we found now is that there was a whole program associated with Cambridge University where a number of researchers, not just Aleksandr Kogan—although to our current knowledge, he is the only one who sold the data to Cambridge Analytica.

There were a number of other researchers who were building similar apps. So we do need to understand whether there is something bad going on at Cambridge University overall that will require a stronger action from us.

Mr. ENGEL. You mentioned before in your remarks hate speech. We have seen the scale and reach of extremism balloon in the last decade, partially because of the expansion of social platforms, whether it is a white supremacist rally in Charlottesville that turned violent or to ethnic cleansing in Burma that resulted in the second largest refugee crisis in the world.

Are you aware of any foreign or domestic terrorist organizations, hate groups, criminal networks, or other extremist networks that have scraped Facebook user data? And if they have and if they do it in the future, how would you go about getting it back or deleting it?

Mr. ZUCKERBERG. Congressman, we are not aware of any specific groups like that that have engaged in this. We are, as I have said, conducting a full investigation of any apps that had access to a large amount of data, and if we find anything suspicious, we will tell everyone affected.

We do not allow hate groups on Facebook overall. So, if there is a group that their primary purpose or a large part of what they do is spreading hate, we will ban them from the platform overall.

Mr. ENGEL. So do you adjust your algorithms to prevent individuals interested in violence or nefarious activities from being connected with other like-minded individuals?

Mr. ZUCKERBERG. Sorry. Could you repeat that?

Mr. ENGEL. Do you adjust your algorithms to prevent individuals interested in violence or bad activities from being connected with other like-minded individuals?

Mr. ZUCKERBERG. Congressman, yes. That is certainly an important thing that we need to do.

Mr. ENGEL. OK. And, finally, let me say this: Many of us are very angry about Russian influence in the 2016 Presidential elections and Russian influence over our Presidential elections.

Does Facebook have the ability to detect when a foreign entity is attempting to buy a political ad, and is that process automated? Do you have procedures in place to inform key Government players when a foreign entity is attempting to buy a political ad or when it might be taking other steps to interfere in an election?

Mr. ZUCKERBERG. Congressman, yes. This is an extremely important area. After we were slow to identify the Russian information operations in 2016, this has become a top priority for our company to prevent that from ever happening again, especially this year in 2018, which is such an important election year with the U.S. midterms, but also major elections in India, Brazil, Mexico, Hungary, Pakistan, a number of other places.

So we are doing a number of things that I am happy to talk about or follow up with afterwards around deploying new AI tools that can proactively catch fake accounts that Russia or others might create to spread misinformation.

And one thing that I will end on here, just because I know we are running low on time, is, since the 2016 election, there have been a number of significant elections, including the French Presidential election, the German election, and last year the U.S. Senate Alabama special election.

And the AI tools that we deployed in those elections were able to proactively take down tens of thousands of fake accounts that may have been trying to do the activity that you are talking about. So our tools are getting better.

For as long as Russia has people who are employed who are trying to perpetrate this kind of interference, it will be hard for us to guarantee that we are going to fully stop everything. But it is an arms race, and I think that we are making ground and are doing better and better and are confident about how we are going to be able to do that.

Mr. WALDEN. The gentleman's time has expired.

Mr. ENGEL. Thank you.



Mr. WALDEN. The Chair recognizes the chairman of the Health Subcommittee, Dr. Burgess of Texas, for 4 minutes.

Mr. BURGESS. Thank you, Mr. Chairman.

And thanks to our witness for being here today.

Mr. Chairman, I have a number of articles that I am going to ask unanimous consent to insert into the record. I know I won't have time to get to all of my questions.

Mr. WALDEN. Without objection.

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

Mr. WALDEN. And we put the slide up that you requested.

Mr. BURGESS. And so I am going to be submitting some questions for the record that are referencing these articles: One is, "Friended: How the Obama Campaign Connected With Young Voters," by Michael Scherer; "We Already Know How to Protect Ourselves from Facebook"—and I hope I get this name right—Zeynep Tufekci; and "It's Time to Break Up Facebook" by Eric Wilson, who, in the interest of full disclosure, is a former staffer.

Mr. WALDEN. Without objection.

Mr. BURGESS. And I will be referencing those articles in some written questions.

I consulted my technology guru, Scott Adams, in the form of Dilbert. Going back 21 years ago, when you took the shrink wrap off of a piece of software that you bought, you were automatically agreeing to be bound by the terms and conditions. So we have gone a long way from taking the shrink wrap off of an app.

But I don't know that things have changed all that much. I guess, does Facebook have a position that you recommend for elements of a company's terms and conditions that you encourage consumers to look at before they click on the acceptance?

Mr. ZUCKERBERG. Congressman, yes. I think that it is really important for this service that people understand what they are doing and signing up for and how this service works. We have laid out all of what we do in the terms of service because that is what is legally required of us. But—

Mr. BURGESS. Let me just ask you, because we are going to run short on time, have you laid out for people what it would be indicative of a good actor versus a less-than-good actor in someone who has developed one of these applications?

Mr. ZUCKERBERG. Congressman, yes. We have a developer terms of service, which is separate from the normal terms of service for individuals using the service.

Mr. BURGESS. Is the average consumer able to determine what elements would indicate poor or weak consumer protections just by their evaluation of the terms and conditions? Do you think that is possible?

Mr. ZUCKERBERG. Congressman, I am not sure what you mean by that.

Mr. BURGESS. Well, can the average person, the average layperson look at the terms and conditions and make the evaluation, is this a strong enough protection for me to enter into this arrangement?

Look, I am as bad as anyone else. I see an app. I want it. I download it. I breeze through the stuff. Just take me to the good

stuff in the app. But if a consumer wanted to know, could they know?

Mr. ZUCKERBERG. Congressman, I think you are raising an important point, which is that I think if someone wanted to know, they could. But I think that a lot of people probably just accept terms of service without taking the time to read through it.

I view our responsibility not as just legally complying with laying it out and getting that consent but actually trying to make sure that people understand what is happening throughout the product.

That is why every single time that you share something on Facebook or one of our services, right there is a control in line where you control who you want to share with. Because I don't just think that this is about a terms of service. It is contextual. You want to present people with the information about what they might be doing and give them the relevant controls in line at the time that they are making those decisions, not just have it be in the background sometime or upfront make a one-time decision.

Mr. BURGESS. Yes. Let me move onto something else. Mr. Pallone brought up the issue of he wanted to see more regulation. We actually passed a bill through this committee last Congress dealing with data breach notification, not so much for Facebook but for the credit card breaches, a good bill.

Many of the friends on the other side of the dais voted against it, but it was Mrs. Blackburn's bill, and I think it is one we should consider again in light of what is going on here.

But you also signed a consent decree back in 2011. And, you know, when I read through that consent decree, it is pretty explicit. And there is a significant fine of \$40,000 per violation per day, and if you have got 2 billion users, you can see how those fines would mount up pretty quickly.

So, in the course of your audit, are you extrapolating data for the people at the Federal Trade Commission for the terms and conditions of the consent decree?

Mr. WALDEN. That is time.

Mr. ZUCKERBERG. That is—I am not sure what you mean by extrapolating data.

Mr. BURGESS. Well, you have referenced there are audits that are ongoing. Are you making that information from those audits available to our friends at the agency, at the Federal Trade Commission?

Mr. ZUCKERBERG. Congressman, as you know, the FTC is investigating this, and we are certainly going to be complying with them and working with them on that investigation.

Mr. WALDEN. The gentleman's time has expired.

The Chair recognizes the gentleman from Texas, Mr. Green, for 4 minutes.

Mr. GREEN. Thank you, Mr. Chairman.

And welcome to our committee.

I want to follow up on what my friend from north Texas talked about on his cartoon. Next month, the general data protection regulation, the GDPR, goes into effect in the European Union. The GDPR is pretty prescriptive on how companies treat consumer data, and it makes it clear that consumers need to be in control of their own data.

Mr. Zuckerberg, Facebook has committed to abiding to these consumer protections in Europe, and you face large penalties if they don't. In recent days, you have said that Facebook intends to make the same settings available to users everywhere, not only in Europe.

Did I understand correctly that Facebook would not only make the same settings available but that it will make the same protections available to Americans that they will to Europeans?

Mr. ZUCKERBERG. Yes, Congressman. All the same controls will be available around the world.

Mr. GREEN. And you commit today that Facebook will extend the same protections to Americans that European users will receive under the GDPR?

Mr. ZUCKERBERG. Yes, Congressman. We believe that everyone around the world deserves good privacy controls. We have had a lot of these controls in place for years. The GDPR requires us to do a few more things, and we are going to extend that to the world.

Mr. GREEN. There are many requirements in the GDPR, so I am just going to focus on a few of them. The GDPR requires that the company's request for user consent to be requested in a clear and concise way, using language that is understandable, and be clearly distinguishable from other pieces of information including terms and conditions. How will that requirement be implemented in the United States?

Mr. ZUCKERBERG. Congressman, we are going to put at the top of everyone's app when they sign in a tool that walks people through the settings and gives people the choices and asks them to make decisions on how they want their settings set.

Mr. GREEN. One of the GDPR's requirements is data portability. Users must be able to permit it to request a full copy of their information and be able to share that information with any companies that they want to.

I know Facebook allows users in the U.S. to download their Facebook data. Does Facebook plan to use the currently existing ability of users to download their Facebook data as the means to comply with the GDPR's data portability requirement?

Mr. ZUCKERBERG. Congressman, I think we may be updating it a little bit. But as you say, we have had the ability to download your information for years now, and people have the ability to see everything that they have in Facebook, to take that out, delete their account, and move their data anywhere that they want.

Mr. GREEN. Does that download file include all the information Facebook has collected about any given individual? In other words, if I download my Facebook information, is there other information accessible to you within Facebook that I wouldn't see on that document, such as browsing history or other inferences that Facebook has drawn from users for advertising purposes?

Mr. ZUCKERBERG. Congressman, I believe all of your information is in that file.

Mr. GREEN. OK. GDPR also gives users the right to object to the processing of their personal data for marketing purposes, which, according to Facebook's website, includes custom microtargeting audiences for advertising. Will the same right to object be available

to Facebook users in the United States, and how will that be implemented?

Mr. ZUCKERBERG. Congressman, I am not sure how we are going to implement that yet. Let me follow up with you on that.

Mr. GREEN. OK. Thank you, Mr. Chairman.

And, again, as a small—Facebook conducted a couple of years ago an effort in our district in Houston for our small businesses, and it was one of the most successful outreach I have seen. So I appreciate that outreach to helping small businesses use Facebook to market their products.

Thank you, Mr. Chairman.

Mr. WALDEN. I thank the gentleman. The Chair now recognizes the gentlelady from Tennessee, Mrs. Blackburn for 4 minutes.

Mrs. BLACKBURN. Thank you, Mr. Chairman. Mr. Zuckerberg, I tell you, I think your cozy community, as Dr. Mark Jameson recently said is beginning to look a whole lot like the Truman Show where people's identities and relationships are made available to people that they don't know and then that data is crunched and it is used, and they are fully unaware of this.

So I have got to ask you I think what we are getting to here is who owns the virtual you? Who owns your presence online? And I would like for you to comment. Who do you think owns an individual's presence online? Who owns their virtual you? Is it you or is it them?

Mr. ZUCKERBERG. Congresswoman, I believe that everyone owns their own content online, and that is the first line of our terms of service, if you read, it says that.

Mrs. BLACKBURN. And where does privacy rank as a corporate value for Facebook?

Mr. ZUCKERBERG. Congresswoman, giving people control of their information and how they want to set their privacy is foundational to the whole service. It is not just kind of an add-on feature, it is something we have to comply with. The reality is if you have a photo—if you just think about this in your day-to-day life—

Mrs. BLACKBURN. I can't let you filibuster right now. A constituent of mine who is a benefits manager brought up a great question in a meeting at her company last week, and she said, you know, healthcare you have got HIPPA, you have got Gramm-Leach-Bliley, you have got the Fair Credit Reporting Act, these are all compliance documents for privacy for other sectors of the industry. She was stunned, stunned that there are no privacy documents that apply to you all.

And we have heard people say that, you know, and you have said you are considering maybe you need more regulation. What we think is we need for you to look at new legislation, and you are hearing there will be more bills brought out in the next few weeks, but we have had a bill, the BROWSER Act, and I am certain that you are familiar with this. It is bipartisan, and I thank Mr. Lipinski, and Mr. Lance, and Mr. Flores for their good work on this legislation. We have had it for over a year, and certainly we have been working on this issue for about 4 years.

And what this would do is have one regulator, one set of rules for the entire ecosystem. And will you commit to working with us

to pass privacy legislation, to pass the BROWSER Act, will you commit to doing that?

Mr. ZUCKERBERG. Congresswoman, I am not directly familiar with the details of what you just said, but I certainly think that regulation in this area—

Mrs. BLACKBURN. OK. Let's get familiar with the details. As you have heard, we need some rules and regulations. This is only 13 pages. The BROWSER Act is 13 pages, so you can easily become familiar with it, and we would appreciate your help.

And I have got to tell you, as Mr. Green just said, as you look at the EU privacy policies, you are already doing much of that. If you are doing everything you claim because you will have to allow consumers to control their data to change, to erase it, you have to give consumers opt-in. So that mothers know—my constituents in Tennessee want to know that they have a right to privacy, and we would hope that that is important to you all.

I want to move on and ask you something else, and please get back to me once you have reviewed the BROWSER Act, I would appreciate hearing from you.

We have done one hearing on algorithms. I chair the Communications and Technology Subcommittee here. We are getting ready to do a second one on algorithms. We are going to do one next week on prioritization, so I would like to ask you: Do you subjectively manipulate your algorithms to prioritize or censor speech?

Mr. ZUCKERBERG. Congresswoman, we don't think about what we are doing as censoring speech. I think that there are types of content like terrorism that I think that we all agree we do not want to have on our service, so we build systems that can identify those and can remove that content, and we are very proud of that. We are—

Mrs. BLACKBURN. Let me tell you something right now. Diamond and Silk is not terrorism.

Mr. WALDEN. The gentlelady's time has expired. The Chair recognizes the gentlelady from Colorado, Ms. DeGette, for 4 minutes.

Ms. DEGETTE. Thank you very much, Mr. Chairman.

Mr. Zuckerberg, we appreciate your contrition and we appreciate your commitment to resolving these past problems. From my perspective, though, and my colleagues' on both sides of the aisle in this committee, we are interested in looking forward to preventing this kind of activity not just with Facebook but with others in your industry, and as has been noted by many people already, we have been relying on self-regulation in your industry, for the most part. We are trying to explore what we can do to prevent further breaches.

So I want to ask you a whole series of fairly quick questions. They should only require yes or no answers. Mr. Zuckerberg, at the end of 2017 Facebook had a total shareholder equity of just over \$74 billion. Is that correct?

Mr. ZUCKERBERG. Sorry, Congresswoman, I am not familiar—

Ms. DEGETTE. At the end of 2017 Facebook had a total shareholder equity of over \$74 billion. Correct?

Mr. ZUCKERBERG. Of over that?

Ms. DEGETTE. That is correct. You are the CEO.

Mr. ZUCKERBERG. The market cap of the company was greater than that, yes.

Ms. DEGETTE. Greater than 74. Last year, Facebook earned a profit of \$15.9 billion on \$40.7 billion in revenue, correct? Yes or no.

Mr. ZUCKERBERG. Yes.

Ms. DEGETTE. Now, since the revelations surrounding Cambridge Analytica, Facebook has not noticed a significant increase in users deactivating their accounts. Is that correct?

Mr. ZUCKERBERG. Yes.

Ms. DEGETTE. Now, since the revelations surrounding Cambridge Analytica, Facebook has also not noticed a decrease in user interaction on Facebook, correct?

Mr. ZUCKERBERG. Yes, that is correct.

Ms. DEGETTE. OK. Now, I want to take a minute to talk about some of the civil and regulatory penalties that we have been seeing. I am aware of two class-action lawsuits that Facebook has settled relating to privacy concerns. Lane versus Facebook was settled in 2010. That case resulted in no money being awarded to Facebook users. Is that correct?

Mr. ZUCKERBERG. Congresswoman, I am not familiar with the details of that.

Ms. DEGETTE. You are the CEO of the company, correct?

Mr. ZUCKERBERG. Yes.

Ms. DEGETTE. Now, this major lawsuit was settled. Do you know about the lawsuit?

Mr. ZUCKERBERG. Congresswoman, I get briefed on these.

Ms. DEGETTE. Do you know about this lawsuit, Lane versus Facebook, yes or no?

Mr. ZUCKERBERG. I am not familiar with the details.

Ms. DEGETTE. OK. If you can supplement. I will just tell you there was this lawsuit, and the users got nothing.

In another case, Fraley versus Facebook, it resulted in a 2013 settlement fund of \$20 million being established with \$15 individual payment payouts to Facebook users beginning in 2016. Is that correct?

Mr. ZUCKERBERG. Congresswoman, I am not familiar—

Ms. DEGETTE. You don't know about that one, either. OK. Well, I will tell you what happened.

Mr. ZUCKERBERG. I discussed that with our team, but I don't remember the exact details.

Ms. DEGETTE. OK. Now as the result of a 2011 FTC investigation into Facebook's privacy policy, do you know about that one?

Mr. ZUCKERBERG. The FTC investigation?

Ms. DEGETTE. Uh-huh.

Mr. ZUCKERBERG. Yes.

Ms. DEGETTE. OK. You entered into a consent decree with the FTC, which carried no financial penalty for Facebook. Is that correct?

Mr. ZUCKERBERG. Congresswoman, I don't remember if we had a financial penalty.

Ms. DEGETTE. You are the CEO of the company. You entered into a consent decree, and you don't remember if you had a financial—

Mr. ZUCKERBERG. I remember the consent decree. The consent decree is extremely important to how we operate the company.

Mr. ZUCKERBERG. Yes. I would think a financial penalty would be, too.

OK. Well, the reason you probably don't remember it is because the FTC doesn't have the authority to issue financial penalties for first-time violations. The reason I am asking these questions, sir, is because we continue to have these abuses and these data breaches, but at the same time it doesn't seem like future activities are prevented. And so, I think one of the things that we need to look at in the future, as we work with you and others in the industry, is putting really robust penalties in place in case of improper actions. And that is why I asked these questions.

Mr. WALDEN. The gentlelady's time has expired. The Chair recognizes the gentleman from Louisiana, the whip of the House, Mr. Scalise, for 4 minutes.

Mr. SCALISE. Thank you, Mr. Chairman, and, Mr. Zuckerberg, I appreciate you coming here. I know, as some of my other colleagues mentioned, you came here voluntarily, and we appreciate the opportunity to have this discussion, because clearly what your company has been able to do has revolutionized the way that people can connect, and there is a tremendous benefit to our country.

Now it is a worldwide platform, and it has helped create a shortage of computer programmers, so as a former computer programmer, I think we would both agree we need to encourage more people to go into the computer sciences because our country is a world leader thanks to your company and so many others, but it obviously raises questions about privacy, and data, and how the data is shared and what is a user's expectation of where that data goes. So I want to ask a few questions.

First, would you agree we need more computer programmers and people to go into that field.

Mr. ZUCKERBERG. Congressman, yes.

Mr. SCALISE. That is a public service announcement we just made, so I appreciate you joining me in that.

Mr. Shimkus' question, it was really a follow-up to a question yesterday that you weren't able to answer, but it was dealing with how Facebook tracks users especially after they log off. And you had said in relation to Congressman Shimkus' question that there is data mining, but it goes on for security purposes.

So my question would be, Is that data that is mined for security purposes also used to sell as part of the business model?

Mr. ZUCKERBERG. Congressman, I believe that we collect different data for those, but I can follow up on the details of that.

Mr. SCALISE. All right. If you can follow up, I would appreciate that.

Getting into this new realm of content review, I know some of the people that work for Facebook—Campbell Brown said, for example, this is changing our relationship with publishers and emphasizing something that Facebook has never done before. It is having a point of view. And you mentioned the Diamond and Silk example where you, I think, described it as a mistake. Were the people who made that mistake held accountable in any way?

Mr. ZUCKERBERG. Congressman, let me follow up with you on that. That situation developed while I was here preparing to testify, so I do not know the details on that.

Mr. SCALISE. OK. I do want to ask you about a study that was done dealing with the algorithm that Facebook uses to describe what is fed to people, through the news feed, and what they found was after this new algorithm was implemented that there was a tremendous bias against conservative news and content and a favorable bias towards liberal content, and if you can look at that, that shows a 16-point disparity, which is concerning.

I would imagine you are not going to want to share the algorithm itself with us. I would encourage you if you wanted to do that, but who develops the algorithm? I wrote algorithms before, and you can determine whether or not you want to write an algorithm to sort data, to compartmentalize data, but you can also put a bias in if that is the directive.

Was there a directive to put a bias in, and first, are you aware of this bias that many people have looked at, and analyzed, and seen?

Mr. ZUCKERBERG. Congressman, that is a really important question. There is absolutely no directive in any of the changes that we make to have a bias on anything that we do. To the contrary, our goal is to be a platform for all ideas. And—

Mr. SCALISE. And I know we are almost out of time, so if you can go back and look and determine if there was a bias whoever developed that software. You have 20,000 people that work on some of this data analysis, if you can look and see if there is a bias and let us know if there is and what you are doing about it, because that is disturbing when you see that kind of disparity.

Finally, there has been a lot of talk about Cambridge and what they have done in the last campaign. In 2008 and 2012, there was also a lot of this done. One of the lead digital heads of the Obama campaign said recently, “Facebook was surprised we were able to suck out the whole social graph, but they didn’t stop us once they realized that was what we were doing. They came to the office in the days following the election recruiting and were very candid that they allowed us to do things they wouldn’t have allowed someone else to do because they were on our side.”

That is a direct quote from one of the heads of the Obama digital team. What would she mean by “they”—Facebook—“were on our side”?

Mr. ZUCKERBERG. Congressman, we didn’t allow the Obama campaign to do anything that any developer on the platform wouldn’t have otherwise been able to do.

Mr. SCALISE. So she was making an inaccurate statement in your point of view?

Mr. ZUCKERBERG. Yes.

Mr. SCALISE. I appreciate the comments, and I look forward to those answers. I yield back the balance of my time.

Mr. WALDEN. The Chair now recognizes the gentleman from Pennsylvania, Mr. Doyle, for 4 minutes.

Mr. DOYLE. Thank you, Mr. Chairman. Mr. Zuckerberg, welcome. Facebook uses some of the most advanced data processing techniques and technologies on the planet, correct?



Mr. ZUCKERBERG. Congressman, we pride ourselves on doing good technical work.

Mr. DOYLE. Thank you. And you use these technologies to flag spam, identify offensive content, and track user activity, right?

Mr. ZUCKERBERG. Among other things.

Mr. DOYLE. But 2015, when the Guardian first reported on Cambridge Analytica using Facebook user data, was that the first time Facebook learned about these allegations?

Mr. ZUCKERBERG. Congressman, in 2015 when we heard that the developer on our platform Aleksandr Kogan—

Mr. DOYLE. Was that the first time you heard about it, when it was reported by the Guardian?

Mr. ZUCKERBERG. That the Guardian reported to Cambridge Analytica?

Mr. DOYLE. When the Guardian made the report, was that the first time you heard about it?

Mr. ZUCKERBERG. Yes.

Mr. DOYLE. Thank you. So do you routinely learn about these violations through the press?

Mr. ZUCKERBERG. Congressman, sometimes we do. I generally think that—

Mr. DOYLE. Let me ask you this. You had the capability to audit developers' use of Facebook user data and do more to prevent these abuses. But the problem at Facebook not only persisted, it proliferated. In fact, relative to other types of problems you had on your platform, it seems as though you turned a blind eye to this, correct?

Mr. ZUCKERBERG. Congressman, I disagree with that assessment. I do think that going forward we need to take a more proactive view of policing what the developers do. Looking back, we have had an app review process. We investigate—

Mr. DOYLE. But, Mr. Zuckerberg, it seems like you were more concerned with attracting and retaining developers on your platform than you were with ensuring the security of Facebook's user data.

Let me switch gears. Your company is subject to a 20-year consent decree with the FTC since 2011, correct?

Mr. ZUCKERBERG. Congressman, we have a consent decree, yes.

Mr. DOYLE. And that decree emerged out of a number of practices that Facebook engaged in that the FTC deemed to be unfair and deceptive. One such practice was making Facebook users' private information public without sufficient notice or consent, claiming that Facebook certified the security and integrity of certain apps when, in fact, it did not, and enabling developers to access about a user and their friends. Is that correct?

Mr. ZUCKERBERG. Congressman, I am not familiar with all of the things that the FTC said, although I am very familiar with the consent order itself.

Mr. DOYLE. But these were part of the FTC consent decree. So I think—I am just concerned that, despite this consent decree, Facebook allowed developers access to an unknown number of user profiles on Facebook for years—potentially hundreds of million, potentially more, and not only allowed but partnered with individuals and app developers such as Aleksandr Kogan, who turned around

and sold that data on the open market and to companies like Cambridge Analytica.

Mr. ZUCKERBERG, you have said that you planned to audit tens of thousands of developers that may have improperly harvested Facebook user data. You also said that you planned to give all Facebook users access to some user controls that will be made available in the EU under the GDPR.

But it strikes me that there is a real trust gap here. This developer data issue is just one example, but why should we trust you to follow through on these promises when you have demonstrated repeatedly that you are willing to flout both your own internal policies and Government oversight when the need suits you?

Mr. ZUCKERBERG. Congressman, respectfully, I disagree with that characterization. We have had a review process for apps for years. We have had reviewed tens of thousands of apps a year and taken action against a number of them. Our process was not enough to catch a developer—

Mr. DOYLE. I see my time is almost over. I just want to say, Mr. Chairman, to my mind the only way we are going to close this trust gap is through legislation that creates and empowers a sufficiently resourced expert oversight agency with rulemaking authority to protect the digital privacy and ensure that companies protect our users' data.

With that, I yield back.

Mr. WALDEN. The gentleman's time has expired. The Chair recognizes the chairman of the Subcommittee on Digital Commerce and Consumer Protection, Mr. Latta of Ohio, for 4 minutes.

Mr. LATTA. Well, thank you Mr. Chairman and, Mr. Zuckerberg, thanks very much for being with us today.

First question I have is can you tell the Facebook users that the Russians and the Chinese have not used the same methods as other third parties to scrape the entire social network for their gain?

Mr. ZUCKERBERG. Congressman, we have not seen that activity.

Mr. LATTA. None at all?

Mr. ZUCKERBERG. Not that I am aware of.

Mr. LATTA. OK. Let me ask this question, you know, it has been going on when you made your opening statement in regards to what you would like to see done with the company and steps moving forward. There has been a couple questions, you know, about you are going to be investigating the apps. How many apps are there out there that you would have to investigate?

Mr. ZUCKERBERG. There are tens of thousands of apps that had access to a large amount of people's information before we locked down the platform in 2014. So we are going to do an investigation that first involves looking at their patterns of API access and what those companies were doing and then if we find anything suspicious then we are going to bring in third-party auditors to go through their technical and physical systems to understand what they did, and if we find that they misused any data then we will ban them from our platform, make sure they delete the data and tell everyone affected.

Mr. LATTA. Just to follow up on that then, how long would it take then to investigate each of those apps once you are doing that be-

cause, again, when you are talking about tens of thousands and you are going through that entire process then how long would it take to go through each one of those apps?

Mr. ZUCKERBERG. Yes, Congressman. It is going to take many months to do this full process.

Mr. LATTA. OK.

Mr. ZUCKERBERG. And it is going to be an expensive process with a lot of auditors, but we think that this is the right thing to do at this point. You know, before we had thought that when developers told us that they weren't going to sell data that that was—that that was a good representation, but one of the big lessons that we have learned here is that clearly we cannot just take the developers' word for it, we need to go in and enforce that.

Mr. LATTA. OK. We are talking about audits. There has been some questions about this on the audits. In 2011 Facebook signed did sign that consent order with the Federal Trade Commission for the privacy violations. Part of that consent order requires Facebook to submit third-party privacy audits to the FTC every 2 years.

First, are you aware of the audits? And, second, why didn't the audits disclose or find these issues with the developers' access to users' data?

Mr. ZUCKERBERG. Yes, Congressman. I am aware of the audits that we do. We do audits every other year. They are ongoing. The audits have not found material issues with our privacy programs in place at the company. I think the broader question here is we have had this FTC consent decree, but we take a broader view of what our responsibility for people's privacy is, and our view is that this—what a developer did that they represented to us that they were going to use the data in a certain way and then in their own systems went out and sold it we do not believe is a violation of the consent decree, but it is clearly a breach of people's trust, and the standard that we hold ourselves to is not just following the laws that are in place, but we also—we just want to take a broader view of this in protecting people's information.

Mr. LATTA. Let me we are just about out of time here. Are you aware that Facebook did provide the auditors all the information it requested when doing the FTC audits?

Mr. ZUCKERBERG. Sorry, can you repeat that?

Mr. LATTA. Yes. Did Facebook provide the auditors all the information requested when preparing the audit for the FTC?

Mr. ZUCKERBERG. Congressman, I believe we do provide the audits to the FTC.

Mr. LATTA. OK. So all the information is provided. And were you ever personally asked to provide information or feedback in these audits to the FTC?

Mr. ZUCKERBERG. Congressman, not personally, although I am briefed on all of the audits by our team.

Mr. LATTA. OK. Mr. Chairman, my time has expired, and I yield back.

Mr. WALDEN. The gentleman yields back. The Chair recognizes the gentlelady from Illinois, Ms. Schakowsky, for 4 minutes.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. You know, you have a long history of growth and success, but you also have a long list of apologies in 2003. It started at Harvard. "I apologize for any

harm done as a result of my neglect.” 2006, “We really messed this one up.” 2007, “We simply did a bad job. I apologize for it.” 2010, “Sometimes we move too fast.” 2011, “I am the first to admit that we have made a bunch of mistakes.” 2017, this is in connection with the Russian manipulation of the election and the data that came from Facebook initially. “I ask for forgiveness. I will work to do better.” So it seems to me from this history that self-regulation, this has proved to me that self-regulation simply does not work.

I have a bill, The Secure and Protect Americans Data Act that I hope you will take a look at, very simple bill about setting standards for how you have to make sure that the data is protected, deadlines on when you have to release that information to the public. Certainly it ought to go to the FTC, as well.

But in response to the questions about the apps and the investigation that you are going to do you said you don’t necessarily know how long. Have you set any deadline for that because we know, as my colleagues said, that there are tens of thousands, there is actually been nine million apps. How long do we have to wait for that kind of investigation?

Mr. ZUCKERBERG. Congresswoman, we expect it to take many months.

Ms. SCHAKOWSKY. Years?

Mr. ZUCKERBERG. I hope not.

Ms. SCHAKOWSKY. OK. I want to ask you, yesterday following up on your response to Senator Baldwin’s question you said yesterday that Kogan also sold data to other firms. You named Eunoia Technologies. How many are there total, and what are their names? Can we get that, and how many are there total?

Mr. ZUCKERBERG. Congresswoman, we can follow up with you to make sure you get all that information.

Ms. SCHAKOWSKY. Yes, but order of magnitude.

Mr. ZUCKERBERG. I don’t believe it was a large number, but as we complete the audits we will know more.

Ms. SCHAKOWSKY. What is a large number?

Mr. ZUCKERBERG. A handful.

Ms. SCHAKOWSKY. Has Facebook tried to get those firms to delete user data and its derivatives?

Mr. ZUCKERBERG. Yes, Congresswoman. In 2015 when we first learned about it we immediately demanded that the app developer and the firms that he sold it to delete the data, and they all represented to us that they had. It wasn’t until about a month ago that new reports surfaced that suggested that they hadn’t, which is what has kicked us off needing to now go do this full audit and investigation and investigate all these other apps that have come up.

Ms. SCHAKOWSKY. Were derivatives deleted?

Mr. ZUCKERBERG. Congresswoman, we need to complete the investigation and audit before I can confirm that.

Ms. SCHAKOWSKY. You are looking into it?

Mr. ZUCKERBERG. What they represented to us is that they have, but we now need to get into their systems and confirm that before I want to stand up here confidently and say what they have done.

Ms. SCHAKOWSKY. So Mr. Green asked about the general data protection regulation on May 25th that is going to go into effect by

the EU, and your response was—let me ask, is your response that exactly the protections that are guaranteed not the—what did you say? Yes, not to condescend the controls but all the rights that are guaranteed under the general data protection regulations will be applied to Americans, as well?

Mr. ZUCKERBERG. Congresswoman, the GDPR has a bunch of different important pieces. One is around offering controls over every use of people's—

Ms. SCHAKOWSKY. Right, that is one. Uh-huh.

Mr. ZUCKERBERG. That we are doing. The second is around pushing for affirmative consent and putting a control in front of people that walks people through their choices.

Ms. SCHAKOWSKY. Exactly.

Mr. ZUCKERBERG. We are going to do that too.

The second, although that might be different depending on the laws in specific countries and different places, but we are going to put a tool at the top of everyone's app that walks them through their settings and helps them understand what is—

Ms. SCHAKOWSKY. It sounds like it will not be exact. And let me say, as we look at—

Mr. WALDEN. The gentlelady's time—

Ms. SCHAKOWSKY [continuing]. The distribution of information that who is going to protect us from Facebook is also a question.

Thank you, and I yield back.

Mr. WALDEN. The gentlelady's time has expired.

The Chair recognizes the gentlelady from Washington State, the Conference chairman.

Mrs. MCMORRIS RODGERS. Thank you.

And thank you, Mr. Zuckerberg, for joining us.

Today's clearly timely. There is a number of extremely important questions Americans have about Facebook, including questions about safety and security of their data, about the process by which their data is made available to third parties, about what Facebook is doing to protect consumer privacy as we move forward.

But one of the issues that is concerning me and I would like to dig a little deeper into is how Facebook treats content on its platform.

So, Mr. Zuckerberg, given the extensive reach of Facebook and its widespread use as a tool of public expression, do you think Facebook has a unique responsibility to ensure that it has clear standards regarding the censorship of content on its platform? And do you think Facebook adequately and clearly defines what these standards are for its users?

Mr. ZUCKERBERG. Congresswoman, yes, I feel like we have a very important responsibility to outline what the content policies are and the community standards are.

This is one of the areas that, frankly, I am worried we are not doing a good enough job at right now, especially because, as an American-based company where about 90 percent of the people in our community are outside of the U.S., where there are different social norms and different cultures, it is not clear to me that our current situation of how we define community standards is going to be effective for articulating that around the world.

So we are looking at different ways to evolve that, and I think that this is one of the more important things that we will do.

Mrs. MCMORRIS RODGERS. OK.

And even focusing on content for here in America, I would like to shift gears just a little bit to talk about Facebook's recent changes to its news feed algorithm.

Your head of news partnerships recently said that Facebook is, quote, "taking a step to define what quality news looks like and give that a boost so that overall there is less competition from news."

Can you tell me what she means by "less competition from news"? And, also, how does Facebook objectively determine what is acceptable news and what safeguards exist to ensure that, say, religious or conservative content is treated fairly?

Mr. ZUCKERBERG. Yes, Congresswoman. I am not sure specifically what that person was referring to, but I can walk you through what the algorithm change was, if that is useful.

Mrs. MCMORRIS RODGERS. Well, maybe I will just go on to my other questions then.

There is an issue of content discrimination, and it is not a problem unique to Facebook. There is a number of high-profile examples of edge providers engaging in blocking and censoring religious and conservative political content. In November, FCC Chairman Pai even said that edge providers routinely block or discriminate against content they don't like.

This is obviously a serious allegation. How would you respond to such an allegation? And what is Facebook doing to ensure that its users are being treated fairly and objectively by content reviewers?

Mr. ZUCKERBERG. Congresswoman, the principle that we are a platform for all ideas is something that I care very deeply about. I am worried about bias, and we take a number of steps to make sure that none of the changes that we make are targeted in any kind of biased way. And I would be happy to follow up with you and go into more detail on that, because I agree that this is a serious issue.

Mrs. MCMORRIS RODGERS. Over Easter, a Catholic university's ad with a picture of the historic San Damiano Cross was rejected by Facebook. Though Facebook addressed the error within days, that it happened at all is deeply disturbing.

Could you tell me what was so shocking, sensational, or excessively violent about the ad to cause it to be initially censored? Given that your company has since said it did not violate terms of service, how can users know that their content is being viewed and judged accordingly to objective standards?

Mr. ZUCKERBERG. Congresswoman, it sounds like we made a mistake there, and I apologize for that. And, unfortunately, with the amount of content in our systems and the current systems that we have in place to review, we make a relatively small percent of mistakes in content review but that is too many, and this is an area where we need to improve.

What I will say is that I wouldn't extrapolate from a few examples to assuming that the overall system is biased. I get how people can look at that and draw that conclusion, but I don't think that

that reflects the way that we are trying to build the system or what we have seen.

Mr. WALDEN. The gentlelady's—

Mrs. MCMORRIS RODGERS. Thank you. And I just—this is an important issue in building trust.

Mr. ZUCKERBERG. I agree.

Mrs. MCMORRIS RODGERS. And that is going to be important.

Thank you, and I yield back.

Mr. WALDEN. The gentlelady's time has expired.

The Chair recognizes the gentleman from North Carolina, Mr. Butterfield, for 4 minutes.

Mr. BUTTERFIELD. Thank you, Mr. Chairman.

And thank you, Mr. Zuckerberg, for your testimony here today.

Mr. Zuckerberg, you have stated that your goal with Facebook is to build strong communities, and certainly that sounds good. You have stated here today on the record that you did not live up to the privacy expectations, and I appreciate that.

But this committee—and you must know this—this committee is counting on you to right a wrong, and I hope you get it. In my opinion, Facebook is here to stay, and so you have an obligation to protect the data that you collect and the data that you use. And Congress has the power to regulate your industry, and we have the power to penalize misconduct.

But I want to go in a different direction today, sir. You and your team certainly know how I feel about racial diversity in corporate America. And Sheryl Sandberg and I talk about that all of the time.

Let me ask you this—and the Congressional Black Caucus has been very focused on holding your industry accountable—not just Facebook, your industry—accountable for increasing African-American inclusion at all levels of the industry.

And I know you have a number of diversity initiatives. In 2017, you have increased your black representation from 2 to 3 percent. While this is a small increase, it is better than none.

But this does not nearly meet the definition of building a racially diverse community. CEO leadership—and I have found this to be absolutely true—CEO leadership on issues of diversity is the only way that the technology industry will change.

So will you commit, sir, to convene, personally convene, a meeting of CEOs in your sector—many of them, all of them perhaps, are your friends—and to do this very quickly to develop a strategy to increase racial diversity in the technology industry?

Mr. ZUCKERBERG. Congressman, I think that that is a good idea, and we should follow up on it.

From the conversations that I have with my fellow leaders in the tech industry, I know that this is something that we all understand that the whole industry is behind on, and Facebook is certainly a big part of that issue.

And we care about this not just from the justice angle but because we know that having diverse viewpoints is what will help us serve our community better, which is ultimately what we are here to do. And I think we know that the industry is behind on this and want to—

Mr. BUTTERFIELD. Well, we have talked with you over the years about this, and while there has been some marginal improvement, we must do better than we have done.

Recently, you appointed an African American, our friend Ken Chenault, to our board. And, of course, Erskine Bowles is already on your board, who is also a friend. But we have to concentrate more on board membership for African Americans and also minorities at the entry level within your company.

I was looking at your website a few minutes ago, and it looks like you list five individuals as leadership in your company, but none of them is African American. I was just looking at it. Not only you and Sheryl, but David, Mike, and Chris, that is your leadership team, and this does not reflect America.

Can you improve the numbers on your leadership team to be more diverse?

Mr. ZUCKERBERG. Congressman, this is an issue that we are focused on. We have a broader leadership than just five people. I mean—

Mr. BUTTERFIELD. It is not on your website.

Mr. ZUCKERBERG. I understand that.

Mr. BUTTERFIELD. We can do better than that, Mr. Zuckerberg. We certainly can.

Do you plan to add an African American to your leadership in the foreseeable future? And will you commit that you will continue to work with us, the Congressional Black Caucus, to increase diversity within your company that you are so proud of?

Mr. ZUCKERBERG. Congressman, we will certainly work with you. This is an important issue.

Mr. BUTTERFIELD. We also find that companies' failure to retain black employees contributes to their low presence at technology companies. And there is little transparency in retention numbers.

So will you commit to providing numbers on your retention—that is the big word, “retention”—of your employees disaggregated by race in your diversity update starting this year? Can we get that data? That is the starting point.

Mr. ZUCKERBERG. Congressman, we try to include a lot of important information in the diversity updates. I will go discuss that with my team after I get back from this hearing.

Mr. BUTTERFIELD. I am out of time, sir. I will take this up with your team in another setting. We will be out there in a few weeks.

Thank you. I yield back.

Mr. WALDEN. The gentleman's time has expired.

The Chair now recognizes now the chairman of the Oversight and Investigations Subcommittee, the gentleman from Mississippi, Mr. Harper, for 4 minutes.

Mr. HARPER. Thank you, Mr. Chairman.

Thank you, Mr. Zuckerberg, for being here. And we don't lose sight of the fact that you are a great American success story. It is a part of everyone's life and business, sometimes maybe too often. But I thank you for taking the time to be here.

And our concern is to make sure that it is fair. We worry, because we are looking at possible Government regulation here, certainly this self-governing, which has had some issues, and how you factor that. And, you know, we are trying to keep up with the algo-



rithm changes on how you determine the prioritization of the news feeds, and you look at, well, it needs to be trustworthy and reliable and relevant. Well, who is going to determine that? That also has an impact. And even though you say you don't want the bias, it is dependent upon who is setting what those standards are in that.

And so I want to ask you a couple of questions, if I may. And this is a quote from Paul Grewal, Facebook's VP and general counsel. He said, "Like all app developers, Mr. Aleksandr Kogan requested and gained access to information from people after they chose to download his app."

Now, under Facebook policy in 2013, if Cambridge Analytica had developed the This is Your Digital Life app, they would have had access to the same data they purchased from Mr. Kogan. Would that be correct?

Mr. ZUCKERBERG. Congressman, that is correct. A different developer could have built that out.

Mr. HARPER. OK.

Now, according to PolitiFact.com—and this is a quote—"The Obama campaign and Cambridge Analytica both gained access to huge amounts of information about Facebook users and their friends, and in neither case did the friends of app users consent," close quote.

This data that Cambridge Analytica acquired was used to target voters with political messages, much as the same type of data was used by the Obama campaign to target voters in 2012. Would that be correct?

Mr. ZUCKERBERG. Congressman, the big difference between these cases is that, in the Kogan case, people signed into that app expecting to share the data with Kogan, and then he turned around and, in violation of our policies and in violation of people's expectations, sold it to a third-party firm, to Cambridge Analytica in this case.

Mr. HARPER. Sure.

Mr. ZUCKERBERG. I think that we were very clear about how the platform worked at the time, that anyone could sign into an app, and they would be able to bring their information, if they wanted, and some information from their friends. People had control over that. So, if you wanted, you could turn off the ability to sign into apps or turn off the ability for your friends to be able to bring your information. The platform worked the way that we had designed it at the time at the time.

I think we now know that we should have a more restrictive platform, where people cannot also bring information from their friends and can only bring their own information. But that is the way that the system worked at the time.

Mr. HARPER. And whether in violation of the agreement or not, you agree that users have an expectation that their information would be protected and remain private and not be sold. And so that is something—the reason that we are here today.

And I can certainly understand the general public's outrage if they are concerned regarding the way Cambridge Analytica required their information. But if people are outraged because they used that for political reasons, would that be hypocritical? Shouldn't they be equally outraged that the Obama campaign used the data of Facebook users without their consent in 2012?

Mr. ZUCKERBERG. Congressman, what I think people are rightfully very upset about is that an app developer that people had shared data with sold it to someone else, and, frankly, we didn't do enough to prevent that or understand it soon enough.

Mr. HARPER. Thank you.

Mr. ZUCKERBERG. And now we have to go through and put in place systems that prevent that from happening again and make sure that we have sufficient controls in place in our ecosystem, so, that way, developers can't abuse people's data.

Mr. HARPER. Thank you, Mr. Zuckerberg.

My time has expired. I yield back.

Mr. WALDEN. The gentleman yields back the balance of his time.

The gentlelady from California, Ms. Matsui, is recognized for 4 minutes.

Ms. MATSUI. Thank you, Mr. Chairman.

And welcome, Mr. Zuckerberg. Thank you very much here.

You know, I was just thinking about Facebook and how you developed your platform, first from a social platform amongst friends and colleagues and joining a community. And a lot of that was based upon trust, because you knew your friends, right? But that evolved into this business platform, and one of the pillars still was trust. And I think everyone here would agree that trust is in short supply here, and that is why we are here today.

Now, you have constantly maintained that consumers own the data they provided to Facebook and should have control over it. And I appreciate that, and I just want to understand more about what that means.

To me, if you own something, you ought to have some say about how and when it is used, but, to be clear, I don't just mean pictures, email addresses, Facebook groups, or pages. I understand the data and the information consumers provided to Facebook can be and perhaps is used by algorithms to form assumptions and inferences about users to better target ads to the individuals.

Now, do you believe that consumers actually own their data even when that data has been supplemented by a data broker, assumptions algorithms have made about that user, or otherwise?

And this is kind of the question that Mrs. Blackburn has come up with, our own comprehensive profile, which is kind of our virtual self.

Mr. ZUCKERBERG. Congresswoman, I believe that people own all of their own content.

Where this gets complicated is, let's say I take a photo and I share it with you. Now, is that my photo, or is it your photo? I would take the position that it is our photo, which is why we make it so that I can bring that photo to another app if I want but you can't. But—

Ms. MATSUI. Well, once it gets to the data broker, though—so there are certain algorithms and certain assumptions made. What happens after that?

Mr. ZUCKERBERG. Sorry, can you clarify that?

Ms. MATSUI. Well, what I mean is that, if you supplement this data, you know, you say you are owning it, but you supplement this when other data brokers, you know, use their other algorithms to supplement this and make their own assumptions, then what

happens there? Because that is, to me, somebody else is taking that over. How can you say that we own that data?

Mr. ZUCKERBERG. Congresswoman, all the data that you put in, all the content that you share on Facebook is yours. You control how it is used. You can remove it at any time. You can get rid of your account and get rid of all of it at once. You can get rid of specific things.

Ms. MATSUI. But you can't claw it back once it gets out there, right? I mean, that is really—we might own our own data, but once it is used in advertising, we lose control over it. Is that not right?

Mr. ZUCKERBERG. Congresswoman, I disagree with that, because one core tenet of our advertising system is that we don't sell data to advertisers. Advertisers don't get access to your data.

There is a core misunderstanding about how that system works, which is that—let's say, if you are a shop and you are selling muffins, right, you might want to target people in a specific town who might be interested in baking or some demographic. But we don't send that information to you; we just show the message to the right people.

And that is a really important, I think, common misunderstanding of how this system works.

Ms. MATSUI. Yes, I understand that, but Facebook sells ads based, at least in part, on data users provide to Facebook. That is right. And the more data that Facebook collects, it allows you to better target ads to users or classes of users.

So, even if Facebook doesn't earn money from selling data, doesn't Facebook earn money from advertising based on that data?

Mr. ZUCKERBERG. Yes, Congresswoman, we run ads. The business model is running ads. And we use the data that people put into the system in order to make the ads more relevant, which also makes them more valuable. But what we hear from people is that, if they are going to see ads, they want them to be good and relevant.

Ms. MATSUI. But we are not controlling that data?

Mr. ZUCKERBERG. No, you have complete control over that.

Mr. WALDEN. The gentlelady's time has expired.

As previously agreed, we will now take a 5-minute recess. And committee members and our witness need to plan to be back in about 5 minutes.

We stand in recess.

[Recess.]

Mr. WALDEN. We will call the Energy and Commerce Committee back to order and recognize the gentleman from New Jersey, Mr. Lance, for 4 minutes for purposes of questions.

Mr. LANCE. Thank you very much, Mr. Chairman.

Mr. Zuckerberg, you are here today because you are the face of Facebook. And you have come here voluntarily. And our questions are based upon our concern about what has occurred and how to move forward.

I am sure you have concluded, based upon what we have asked, that we are deeply offended by censoring of content inappropriately by Facebook. Examples have been raised—a Roman Catholic university, a State Senate candidate in Michigan. I would be offended

if this censoring were occurring on the left as well as the right, and I want you to know that.

And do you take from what we have indicated so far that, in a bipartisan fashion, Congress is offended by inappropriate censoring of content?

Mr. ZUCKERBERG. Congressman, yes. This is extremely important. And I think the point that you have raised is particularly important, that we have heard today a number of examples of where we may have made content review mistakes on conservative content, but I can assure you that there are a lot of folks who think that we make content moderation or content review mistakes of liberal content as well.

Mr. LANCE. Fair enough. My point is that we don't favor censoring in any way, so long as it doesn't involve hate speech or violence or terrorism. And, of course, the examples today indicate quite the contrary, number one.

Number two, Congresswoman Blackburn has mentioned her legislation. I am a cosponsor of the BROWSER legislation. I commend it to your attention, to the attention of your company. It is for the entire ecosystem. It is for ISPs and edge providers; it is not just for one or the other. It is an opt-in system, similar to the system that exists in Europe.

Might I respectfully request of you, Mr. Zuckerberg, that you and your company review the BROWSER legislation? And I would like your support for that legislation after your review of it.

Mr. ZUCKERBERG. We will review it and get back to you.

Mr. LANCE. Thank you very much.

Your COO, Sheryl Sandberg, last week appeared on the "Today" program, and she admitted the possibility that additional breaches in personal information could be discovered by the current audits. Quote, "We are doing an investigation. We are going to do the audits. And, yes, we think it is possible. That is why we are doing the audits."

And then the COO went on to say, "Facebook cared about privacy all along, but I think we got the balance wrong."

Do you agree with the statement of your COO?

Mr. ZUCKERBERG. Yes, Congressman, I do.

We were trying to balance two equities: on the one hand, making it so that people had data portability, the ability to bring their data to another app, in order to have new experiences in other places, which I think is a value that we all care about. On the other hand, we also need to balance making sure that everyone's information is protected. And I think that we didn't get that balance right up front.

Mr. LANCE. Thank you. I certainly concur with the statement of the COO, as affirmed by you today, that you got the balance wrong.

And then, regarding Cambridge Analytica, the fact that 300,000 individuals or so gave consent but that certainly didn't mean they gave consent to 87 million friends, do you believe that that action violated your consent agreement with the Federal Trade Commission?

Mr. ZUCKERBERG. We do not believe it did. But, regardless, we take a broader view of what our responsibility is to protect people's privacy. And if a developer who people gave their information to,

in this case Aleksandr Kogan, then goes and, in violation of his agreement with us, sells the data to Cambridge Analytica, that is a big issue. And I think people have a right to be very upset—I am upset that that happened. And we need to make sure that we put in place the systems to prevent that from happening again.

Mr. LANCE. Thank you. I think it may have violated the agreement with the Federal Trade Commission, and I am sure that will be determined in the future.

Thank you, Mr. Chairman.

Mr. WALDEN. I thank the gentleman from New Jersey.

I recognize the gentlelady from Florida, Ms. Castor, for 4 minutes.

Ms. CASTOR. Thank you, Mr. Chairman.

Welcome, Mr. Zuckerberg.

For all of the benefits that Facebook has provided in building communities and connecting families, I think a devil's bargain has been struck. And, in the end, Americans do not like to be manipulated. They do not like to be spied on. We don't like it when someone is outside of our home watching. We don't like it when someone is following us around the neighborhood or, even worse, following our kids or stalking our children.

Facebook now has evolved to a place where you are tracking everyone. You are collecting data on just about everybody.

Yes, we understand the Facebook users that proactively sign in are part of that platform, but you are following Facebook users even after they log off of that platform and application, and you are collecting personal information on people who do not even have Facebook accounts. Isn't that right?

Mr. ZUCKERBERG. Congresswoman, I believe—

Ms. CASTOR. Yes or no?

Mr. ZUCKERBERG. Congresswoman, I am not sure that—I don't think that that is what we are tracking.

Ms. CASTOR. No, you are collecting—you have already acknowledged that you are doing that for security purposes and commercial purposes. So you are collecting data outside of Facebook. When someone goes to a website and it has the Facebook "like" or "share," that data is being collected by Facebook, correct?

Mr. ZUCKERBERG. Congresswoman—

Ms. CASTOR. Yes or no?

Mr. ZUCKERBERG [continuing]. That is right, that we understand, in order to show which of your friends liked a—

Ms. CASTOR. Yes. So for people that don't even have Facebook—I don't think that the average American really understands that today, something that fundamental, and that you are tracking everyone's online activities, their searches. You can track what people buy, correct?

Mr. ZUCKERBERG. Congresswoman—

Ms. CASTOR. You are collecting that data, what people purchase online, yes or no?

Mr. ZUCKERBERG. I actually—if they share it with us. But, Congresswoman, overall—

Ms. CASTOR. Because it has a "share" button, so it is gathering—Facebook has the application—in fact, you patented applications to do just that. Isn't that correct? To collect that data?

Mr. ZUCKERBERG. Congresswoman, I don't think any of those buttons share transaction data.

But, broadly, I disagree with the characterization—

Ms. CASTOR. But they track you. You are collecting medical data, correct, on people that are on the internet, whether they are Facebook users or not? Right?

Mr. ZUCKERBERG. Congresswoman, yes, we collect some data for security purposes and—

Ms. CASTOR. And you watch where we go. Senator Durbin had a funny question yesterday about where you are staying, and you didn't want to share that. But Facebook also gathers that data about where we travel. Isn't that correct?

Mr. ZUCKERBERG. Congresswoman, everyone has control over how that works.

Ms. CASTOR. I am going to get to that, but, yes, you are—would you just acknowledge that, yes, Facebook is—that is the business you are in, gathering data and aggregating that data? Correct?

Mr. ZUCKERBERG. Congresswoman, I disagree with that characterization.

Ms. CASTOR. Are you saying you do not gather data on where people travel based upon their internet and the ways they sign in and things like that?

Mr. ZUCKERBERG. Congresswoman, the primary way that Facebook works is that people choose to share data, and they share content—

Ms. CASTOR. The primary way, but the other way that Facebook gathers data is you buy data from data brokers outside of the platform, correct?

Mr. ZUCKERBERG. Congresswoman, we just announced 2 weeks ago that we were going to stop interacting with data brokers, even though that is an industry norm to make it so that the advertising can be more relevant—

Ms. CASTOR. But I think, in the end, I think what—see, it is practically impossible these days to remain untracked in America, for all the benefits Facebook has brought and the internet. And that is not part of the bargain.

And current laws have not evolved, and the Congress has not adopted laws to address digital surveillance. And Congress should act. And I do not believe that the controls, the opaque agreement, consent agreements—the settings are an adequate substitute for fundamental privacy protections for consumers.

Now—

Mr. WALDEN. The gentlelady's time—

Ms. CASTOR. Thank you. I will yield back my time—

Mr. WALDEN. The gentlelady—

Ms. CASTOR [continuing]. And let that stand. And I would like to ask unanimous consent that I put my constituents' questions in the record for—

Mr. WALDEN. Without objection.

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

Ms. CASTOR. Thank you.

Mr. WALDEN. The Chair now recognizes the gentleman from Kentucky, Mr. Guthrie, for 4 minutes.

Mr. GUTHRIE. Thank you, Mr. Chairman.

Thanks for being here.

When I first got into public office, the internet was really kicking off, and I had a lot of people complain about ads, just the inconvenience of ads, trying to get through in the cumbersome in the internet.

I remember telling someone one time—being from Kentucky, a basketball fan, I said, there is nothing I hate worse than the 4-minute timeout, the TV timeout. It ruins the flow of the game and everything. But because of the 4-minute timeout, I get to watch the game for free. So that is something I am willing to accept to watch for free.

What you are not really willing to accept is that your data is just out there and that it is being used but it is being used in the right way.

And it is funny, because I was going to ask this question anyway. I was planning a family trip to Florida, and I searched a town in Florida, and all of a sudden I started getting ads for a brand of hotel that I typically stay in, at a great hotel, at the price available to the public, because it was on the internet, that I was willing to pay and stay there. And so I thought it was actually convenient. Instead of getting just an ad to someplace I will never go, I got an ad specifically to a place I was looking to go, so I thought that was convenient.

And it wasn't Facebook, although my wife used Facebook to message my mother-in-law this weekend for where we are meeting up. So it is very valuable that we get to do that for free because your business model relies on consumer-driven data. This wasn't Facebook; it was a search engine, but they used consumer-driven data to target an ad to me.

So you are not unique in Silicon Valley or in this internet world in doing this type of targeted ads, are you?

Mr. ZUCKERBERG. No, Congressman. You are right. Ad-based business models have been a common way that people have been able to offer free services for a long time. And our social mission of trying to help connect everyone in the world relies on having a service that can be affordable for everyone, that everyone can use. And that is why the ads business model is in service of the social mission we have. And, you know, I think sometimes that gets lost, but I think that that is a really important point.

Mr. GUTHRIE. But you are different, in that, instead of getting just—when I am watching the Hilltoppers on basketball, the person advertising to me doesn't know anything about me. I am just watching the ad. So there is no data, no agreement, and no risk, I guess, there. But with you, there is consumer-driven data.

But if we were to greatly reduce or stop—or just greatly reduce through legislation the use of consumer-driven data for targeting ads, what do you think that would do to the internet? And when I say "internet," I mean everything, not just Facebook.

Mr. ZUCKERBERG. Well, Congressman, it would make the ads less relevant. So—

Mr. GUTHRIE. If you had less revenue, what would that do to—

Mr. ZUCKERBERG. And, yes, it would reduce—it would have a number of effects.

For people using the services, it would make the ads less relevant to them. For businesses, like the small businesses that use advertising, it would make advertising more expensive, because now they would have to pay more to reach more people inefficiently, because targeting helps small businesses be able to afford and reach people as effectively as big companies have typically had the ability to do for a long time.

It would affect our revenue some amount too, but I think there are a couple of points here that are lost. One is that we already give people the control to not use that data and ads if they want. Most people don't do that. I think part of the reason for that is that people get that if they are going to see ads that they want them to be relevant.

But the other thing is that a lot of what makes the ads work or what makes the business good is just that people are very engaged with Facebook. We have more than a billion people who spend almost an hour a day across all our services.

Mr. GUTHRIE. OK. I have 30 seconds. So I appreciate the answer to that. But if—so I didn't opt out and so forth, and all of a sudden I say, this just doesn't work for me, so I want to delete—you told Congressman Rush that you could delete. What happens to the data? I have already—it is there, it has been used, Cambridge Analytica may have it. So what happens when I say, Facebook, take my data off your platform?

Mr. ZUCKERBERG. If you delete your account, we immediately make it so that your account is no longer available once you are done deleting it, so no one can find you on the service. We wouldn't be able to recreate your account from that.

We do have data centers and systems that are redundant, and we have backups in case something bad happens. And over a number of days, we will go through and make sure that we flush all the content out of the system.

But as soon as you delete your account, effectively, that content is dismantled, and we wouldn't be able to put your account back together if we wanted to.

Mr. WALDEN. The gentleman's time has expired.

Mr. GUTHRIE. Well, thank you. My time has expired. I appreciate it.

Mr. WALDEN. I recognize the gentleman from Maryland, Mr. Sarbanes, for 4 minutes.

Mr. SARBANES. Thank you, Mr. Chairman.

Good morning, Mr. Zuckerberg.

I wanted to get something on the record quickly before I move to some questions. You had suggested in your testimony over the last couple days that Facebook notified the Trump and Clinton campaigns of Russian attempts to hack into those campaigns. But representatives of both campaigns in the last 24 hours have said that didn't happen. So we are going to need to follow up on that and find out what the real story is, but—

Mr. ZUCKERBERG. Do you want me to—

Mr. SARBANES. No. I would like to move on. You can provide a response to that in writing, if you would.



Let me ask you: Is it true that Facebook offered to provide what I guess you referred to as dedicated campaign embeds to both of the Presidential campaigns?

Mr. ZUCKERBERG. Congressman, I can quickly respond to the first point too.

Mr. SARBANES. Just say yes or no. Were there embeds in the two campaigns? Were offers of embeds—

Mr. ZUCKERBERG. Congressman, we—

Mr. SARBANES. Yes or no. Were there embeds offered to the Trump campaign and the Clinton campaign?

Mr. ZUCKERBERG. We offer sales support to every campaign.

Mr. SARBANES. OK. So sales support. I am going to refer to that as embeds. And I gather that Mr. Trump's campaign ultimately accepted that offer. Is that correct? Yes or no.

Mr. ZUCKERBERG. Congressman, the Trump campaign had sales support, and the Clinton campaign had sales support too.

Mr. SARBANES. OK. So they had embeds. I am going to refer to those as embeds. What I would like for you to do, if you could—we are not going to have time for you to do this now—but if you could provide to the committee both the initial offer terms and then any subsequent offer terms that were presented to each candidate in terms of what the embed services would be, that would be very helpful.

Do you know how many ads were approved for display on Facebook for each of the Presidential candidates by Facebook?

Mr. ZUCKERBERG. Congressman, I do not, sitting here, off the top of my head, but—

Mr. SARBANES. OK. Let me tell you what they were, because I do. President Trump's campaign had an estimated 5.9 million ads approved; and Secretary Clinton, 66,000 ads. So that is a delta of about 90 times as much on the Trump campaign, which raises some questions about whether the ad approval processes were maybe not processed correctly or inappropriately bypassed in the final months and weeks of the election by the Trump campaign.

And what I am worried about is that the embeds may have helped to facilitate that. Can you say with absolute certainty that Facebook or any of the Facebook employees working as campaign embeds did not grant any special approval rights to the Trump campaign to allow them to upload a very large number of Facebook ads in that final stretch?

Mr. ZUCKERBERG. Congressman, we apply the same standard to all campaigns.

Mr. SARBANES. Can you say that there were not special approval rights granted? Is that what you are saying? There were not special approval rights granted by any of the embeds or support folks, as you call them, in that Trump campaign?

Mr. ZUCKERBERG. Congressman—

Mr. SARBANES. Yes or no.

Mr. ZUCKERBERG. Yes. What I am saying is that—

Mr. SARBANES. If you are saying yes, then I will take you at your word.

The reason this is important and the reason we need to get to the bottom of it is because it could be a serious problem if these kinds of services were provided beyond what is offered in the nor-

mal course, because that could result in violation of campaign finance law because it would be construed as an in-kind contribution, corporate contribution from Facebook beyond what the sort of ad buy opportunity would typically provide.

The reason I am asking you these questions is because I am worried that that embed program has the potential to become a tool for Facebook to solicit favor from policymakers, and that then creates the potential for real conflict of interest.

And I think a lot of Americans are waking up to the fact that Facebook is becoming sort of a self-regulated super structure for political discourse. And the question is, are we the people going to regulate our political dialogue, or are you, Mark Zuckerberg, going to end up regulating the political discourse? So we need to be free of that undue influence.

I thank you for being here, and I yield back.

Mr. WALDEN. The gentleman's time has expired.

The Chair recognizes the gentleman from Texas, Mr. Olson, for 4 minutes.

Mr. ZUCKERBERG. Mr. Chairman, do you mind for the record if I just answer the first point for—take 10 seconds.

Mr. WALDEN. That is fine. Go ahead.

Mr. ZUCKERBERG. When I was referring to the campaigns yesterday I meant the DNC and RNC. So I may have misspoken and maybe technically that is called the committees, but those were the folks who I was referring to.

Mr. WALDEN. Thank you for that clarification.

We will now go to Mr. Olson from Texas for 4 minutes.

Mr. OLSON. I thank the Chair.

Mr. Zuckerberg, I know we both wish we had met under a different set of circumstances. When the story broke, you were quoted as saying, "I started Facebook. I run it. I am responsible for what happens here," end quote. You said those same words in your opening statement about an hour and a half ago.

I know you believe that in your heart. It is not just some talking points or canned speech. Because of my 4 years—I am sorry—9 years in the Navy, I know the best commanding officers, the best skippers, the best CEOs have that exact same attitude.

If Facebook was a Navy ship, your privacy has taken a direct hit. Your trust is severely damaged. You are taking on water, and your future may be a fine with a number, per The Washington Post, with four commas in it. Today, over a billion dollars in fines come your way. As you know, you have to reinforce your words with actions.

I have a few questions about some anomalies that have happened in the past. First of all, back in 2012, apparently Facebook did the experiment on 689,003 Facebook users: You reduced positive posts from users' friends and limited so-called downer posts from other friends so they see the positive information from one group; and the other group, negative information. The goal was to see how the tone of these posts would affect behavior. I look at this Forbes article, The LA Times about illegal human experimentation without permission. I want to talk about that.

But it seems that this is disconnecting people in stark contrast to your mission to connect people. Explain to us how you guys

thought this idea was a good idea, experimenting with people, giving them more negative information, positive information.

Mr. ZUCKERBERG. Well, Congressman, I view our responsibility as not just building services that people like to use but making sure that those services are also good for people and good for society overall.

At the time, there were a number of questions about whether people seeing content that was either positive or negative on social networks was affecting their mood. And we felt like we had a responsibility to understand whether that was the case because we don't want to have that effect, right.

We don't want it to have it so that—we want use in social media and our products to be good for people's well-being. We continually make changes to that effect. Including just recently, this year, we did a number of research projects that showed that when social media is used for building relationships. So when you are interacting with people, it is associated with a lot of positive effects of well-being that you would expect: It makes you feel more connected, less lonely. It correlates with long-term measures of happiness and health.

Whereas, if you are using social media or the internet just to passively consume content, then that doesn't have those same positive effects or can even be negative. So we have tried to shift the product more towards helping people interact with friends and family as a result of that. So that is the kind of—an example of the kind of work that we do.

Mr. OLSON. One last question. I believe I have heard you employ 27,000 people thereabouts. Is that correct?

Mr. ZUCKERBERG. Yes.

Mr. OLSON. I have also been told that about 20,000 of those people, including contractors, do work on data security. Is that correct?

Mr. ZUCKERBERG. Yes. The 27,000 number is full-time employees, and the security and content review includes contractors, of which there are tens of thousands or will be by the time that—

Mr. OLSON. OK. So roughly at least half your employees are dedicated to security practices. How can Cambridge Analytica happen with so much of your workforce dedicated to these causes? How did that happen?

Mr. ZUCKERBERG. Well, Congressman, the issue with Cambridge Analytica and Aleksandr Kogan happened before we ramped those programs up dramatically. But one thing that I think is important to understand overall is just the sheer volume of content on Facebook makes it that we can't—no amount of people that we can hire will be enough to review all of the content.

We need to rely on and build sophisticated AI tools that can help us flag certain content, and we are getting good in certain areas. One of the areas that I mentioned earlier was terrorist content, for example, where we now have AI systems that can identify and take down 99 percent of the al-Qaida and ISIS-related content in our system before someone, a human, even flags it to us. I think we need to do more of that.

Mr. WALDEN. The gentleman's time has expired.

The Chair recognizes the gentleman from California, Mr. McNerney, for 4 minutes.

Mr. MCNERNEY. I thank the chairman.

Mr. Zuckerberg, I thank you for agreeing to testify before the House and Senate committees. I know it is a long and grueling process, and I appreciate your cooperation.

I am a mathematician that spent 20 years in industry and Government developing technology including algorithms. Moreover, my constituents are impacted by these issues, so I am deeply committed and invested here. I am going to follow up on an earlier question.

Is there currently a place that I can download all of the Facebook information about me, including the websites that I have visited?

Mr. ZUCKERBERG. Yes, Congressman. We have a Download Your Information tool. We have had it for years. You can go to it in your settings and download all of the content that you have on Facebook.

Mr. MCNERNEY. Well, my staff, just this morning, downloaded their information, and their browsing history is not in there. So are you saying that Facebook does not have browsing history?

Mr. ZUCKERBERG. Congressman, that would be correct. If we don't have content in there, then that means that you don't have it on Facebook or you haven't put it there.

Mr. MCNERNEY. So I am not quite on board with this. Is there any other information that Facebook has obtained about me, whether Facebook collected it or obtained it from a third party, that would not be included in the download?

Mr. ZUCKERBERG. Congressman, my understanding is that all of your information is included in Download Your Information.

Mr. MCNERNEY. OK. I am going to follow up with this afterwards.

Mr. Zuckerberg, you indicated that the European users have these GDR protections on May 25 and American users will have those similar protections. When will the American users have those protections?

Mr. ZUCKERBERG. Congressman, we are working on doing that as quickly as possible. I don't have the exact date yet.

Mr. MCNERNEY. So it will not be on May 25?

Mr. ZUCKERBERG. We are working on it.

Mr. MCNERNEY. Thank you.

Your company and many companies with an online presence have a staggering amount of personal information. The customer is not really in the driver's seat about how their information is used or monetized. The data collectors are in the driver's seat.

Today, Facebook is governed by weak Federal privacy protections. I have introduced legislation that would help address these issues. They MY DATA Act would give the FTC rulemaking authority to provide consumers with strong data, privacy, and security protections. Without this kind of legislation, how can we be sure that Facebook won't continue to be careless with users' information?

Mr. ZUCKERBERG. Well, Congressman, let me first just set aside that my position isn't that there should be no regulation.

Mr. MCNERNEY. Correct.

Mr. ZUCKERBERG. But regardless of what the laws are that are in place, we have a very strong incentive to protect people's infor-

mation. This is the core thing that Facebook is, is, about 100 billion times a day, people come to our service to share a photo or share a message or——

Mr. MCNERNEY. I hear you saying this, but the history isn't there. So I think we need to make sure that there are regulations in place to give you the proper motivation to stay in line with data protection.

One of the problems here, in my mind, is that Facebook's history, the privacy—user privacy and security have not been given as high priority as corporate growth, and you have admitted as much. Is Facebook considering changing its management structure to ensure that privacy and security have sufficient priority to prevent these problems in the future?

Mr. ZUCKERBERG. Congressman, this is an incredibly high priority for us. When I was saying before that the core use of the product every day, about 100 billion times, is that people come and try to share something with a specific set of people, that works because people have confidence that, if they send a message, it is going to go to the person that they want. If they want to share a photo with their friends, it is going to go to the people who they want. That is incredibly important. We have built a robust privacy program. We have a chief privacy officer——

Mr. MCNERNEY. That is a little bit off track from what I am trying to get at. The privacy protections clearly failed in a couple of cases that are high profile right now. And part of the blame that seems to be out there is that the management structure for privacy and security don't have the right level of a profile in Facebook to get your attention to make sure that they get the proper resources.

Mr. WALDEN. The gentleman's time has expired.

The Chair recognizes the gentleman from West Virginia, Mr. McKinley, for 4 minutes.

Mr. MCKINLEY. Thank you for coming, Mr. Zuckerberg.

I have got a yes-or-no question, if you could give that. Should Facebook enable illegal online pharmacies to sell drugs such as oxycodone, Percocet, Vicodin without a prescription?

Mr. ZUCKERBERG. Congressman, I believe that is against our policies.

Mr. MCKINLEY. Yes or no, do you think you should be able to do that?

Mr. ZUCKERBERG. No, of course not.

Mr. MCKINLEY. And there are 35,000 online pharmacies operating, and according to the FDA, they think there may be 96 percent of them are operating illegally. And on November of last year, CNBC had an article say that you were surprised by the breadth of this opioid crisis.

And, as you can see from these photographs, opioids are still available on your site, that they are without a prescription on your site. So it contradicts just what you just said just a minute ago.

And it went on last week. FDA Commissioner Scott Gottlieb, has testified before our office, said that the internet firms simply aren't taking practical steps to fine and remove these illegal opioid listings, and he specifically mentioned Facebook. Are you aware of that, his quote?

Mr. ZUCKERBERG. Congressman——

Mr. MCKINLEY. Yes or no.

Mr. ZUCKERBERG [continuing]. I am not specifically aware of his quote, but I heard that he said something. And let me just speak to this for a second, because—

Mr. MCKINLEY. If I could—no. We don't—so, in your opening statement—and I appreciated your remark—you said it is not enough to give people a voice; we have to make sure that people aren't using it, Facebook, to hurt people.

Now, America is in the midst of one of the worst epidemics that it has ever experienced with its drug epidemic. And it is all across this country, not just in West Virginia. But your platform is still being used to circumvent the law and allow people to buy highly addictive drugs without a prescription.

With all due respect, Facebook is actually enabling an illegal activity, and in so doing, you are hurting people. Would you agree with that statement?

Mr. ZUCKERBERG. Congressman, I think that there are a number of areas of content that we need to do a better job policing on our service. Today, the primary way that content regulation works here—and review—is that people can share what they want openly on the service, and then, if someone sees an issue, they can flag it to us, and then we will review it.

Over time, we are shifting to a mode—

Mr. MCKINLEY. You can find out, Mr. Zuckerberg. You know which pharmacies are operating legally and illegally, but you are still continuing to take that—allow that to be posted on Facebook and allow people to get—this scourge, this ravage in this country is being enabled because of Facebook.

So my question to you as we close on this: You have said before you were going to take down those ads, but you didn't do it. We have got statement after statement about things, you are going to take those down within days, and they haven't gone down. That, what I just put up, was just from yesterday. It is still up.

So my question to you is, when are you going to stop—take down these posts that are done with illegal digital pharmacies? When are you going to take them down?

Mr. ZUCKERBERG. Congressman, right now, when people report the posts to us, we will take them down and have people review them.

Mr. MCKINLEY. Why do they have to—if you have got all these 20,000 people, you know that they are up there. Where is your requirement—where is your accountability to allow this to be occurring, this ravage in this country?

Mr. ZUCKERBERG. Congressman, I agree that this is a terrible issue. And, respectfully, when there are tens of billions or 100 billion pieces of content that are shared every day, even 20,000 people reviewing it can't look at everything. What we need to do is build more AI tools that can proactively find that content.

Mr. MCKINLEY. You have said before you were going to take them down, and you haven't.

Mr. WALDEN. The gentleman's time has expired.

The Chair recognizes the gentleman from Vermont, Mr. Welch, for 4 minutes.

Mr. WELCH. Thank you, Mr. Chairman.

Mr. Zuckerberg, you acknowledged candidly that Facebook made a mistake. You did an analysis of how it happened. You promised action. We are at the point where the action will speak much louder than the words.

But, Mr. Chairman, this Congress has made a mistake. This event that happened, whether it was Facebook or some other platform, was foreseeable and inevitable, and we did nothing about it.

Congresswoman Blackburn and I had a group, a privacy working group, six meetings with many of the industry players. There was an acknowledgment on both sides that privacy was not being protected, that there was no reasonable safeguard for Americans' privacy. But there was an inability to come to a conclusion.

So we also have an obligation. And in an effort to move forward, Mr. Zuckerberg, I have framed some questions that hopefully will allow a reasonable yes or no answer to see if there is some common ground to achieve the goal you assert you have, and we certainly have, the obligation to protect the privacy of American consumers.

First, do you believe that consumers have a right to know and control what personal data companies collect from them?

Mr. ZUCKERBERG. Yes.

Mr. WELCH. Do you believe that consumers have a right to control how and with whom their personal information is shared with third parties?

Mr. ZUCKERBERG. Congressman, yes, of course.

Mr. WELCH. And do you believe that consumers have a right to secure and responsible handling of their personal data?

Mr. ZUCKERBERG. Yes, Congressman.

Mr. WELCH. And do you believe that consumers should be able to easily place limits on the personal data that companies collect and retain?

Mr. ZUCKERBERG. Congressman, that seems like a reasonable principle to me.

Mr. WELCH. OK. And do you believe that consumers should be able to correct or delete inaccurate personal data that companies have obtained?

Mr. ZUCKERBERG. Congressman, that one might be more interesting to debate because it depends—

Mr. WELCH. Well, then you get back to us with specifics on that. I think they do have that right.

Do you believe that consumers should be able to have their data deleted immediately from Facebook when they stop using the service?

Mr. ZUCKERBERG. Yes, Congressman, and they have that ability.

Mr. WELCH. Good.

And do you believe that the Federal Trade Commission or another properly resourced governmental agency with rulemaking authority should be able to determine on a regular basis what is considered personal information to provide certainty for consumers and companies what information needs to be protected most tightly?

Mr. ZUCKERBERG. Congressman, I certainly think that that is an area where we should discuss some sort of oversight.

Mr. WELCH. There is not a big discussion here. Who gets the final say? Is it the private market, companies like yours, or is there a governmental function here that defines what privacy is?

Mr. ZUCKERBERG. Congressman, I think that is—this is an area where some regulation makes sense. You proposed a very specific thing, and I think the details matter.

Mr. WELCH. All right. Let me ask you this—I have appreciated your testimony—will you work this committee to help put us—to help the U.S. put in place our own privacy regulation that prioritizes consumers' right to privacy just as the EU has done?

Mr. ZUCKERBERG. Congressman, yes, I will make sure that we work with you to flesh this out.

Mr. WELCH. All right. And you have indicated that Facebook has not always protected the privacy of their users throughout the company's history. And it seems, though, from your answers, that consumers—you agree that consumers do have a fundamental right to privacy that empowers them to control the collection, the use, the sharing of their personal information online. And thank you.

Mr. Chairman, privacy cannot be based just on company policies. Whether it is Facebook or any other company, there has to be a willingness on the part of this Congress to step up and provide policy protection to the privacy rights of every American consumer.

I yield back.

Mr. WALDEN. The gentleman yields back.

The Chair recognizes the gentleman from Illinois, Mr. Kinzinger, for 4 minutes.

Mr. KINZINGER. Thank you, Mr. Chairman.

Mr. Zuckerberg, thank you for being here.

Given the global reach of Facebook, I would like to know about the company's policies and practices with respect to information sharing with foreign governments, if you don't mind. What personal data does Facebook make available from Facebook, Instagram, WhatsApp, to Russian state agencies, including intel and security agencies?

Mr. ZUCKERBERG. Congressman, in general, the way we approach data and law enforcement is if we have knowledge of imminent harm, physical harm that might happen to someone, we try to reach out to local law enforcement in order to help prevent that.

I think that that is less built out around the world. It is more built out in the U.S. So, for example, on that example, we build out specific programs in the U.S. We have 3,000 people that are focused on making sure that if we detect that someone is at risk of harming themselves, we can get them the appropriate help.

Mr. KINZINGER. What about Russian intel agencies?

Mr. ZUCKERBERG. The second category of information is when there is a valid legal process served to us. In general, if a government puts something out that is overly broad, we are going to fight back on it. We view our duty as protecting people's information, but if there is valid service, especially in the U.S., we will, of course, work with law enforcement. In general, we are not in the business of providing a lot of information to the Russian Government.

Mr. KINZINGER. Do you know, is this data only from accounts located in or operated from these individual countries, or does it include Facebook's global data?



Mr. ZUCKERBERG. Sorry. Can you repeat that?

Mr. KINZINGER. Yes. Is the data only from the accounts located in or operated from those countries in terms of Russia or anything, or does it include Facebook's global data?

Mr. ZUCKERBERG. Well, Congressman, in general, countries do not have jurisdiction to have any valid legal reason to request data of someone outside of their country. But—

Mr. KINZINGER. Where is it stored? I mean, do they have access to data—

Mr. ZUCKERBERG. Oh, we don't store any data on Russia.

Mr. KINZINGER. OK. So it is the global data?

Mr. ZUCKERBERG. Yes.

Mr. KINZINGER. So let me just ask, you mentioned a few times that we are in an arms race with Russia, but is it one-sided if Facebook as an American-based company is giving the opposition everything it needs in terms of where it is storing its data?

Mr. ZUCKERBERG. Sorry, Congressman, could you repeat that?

Mr. KINZINGER. So you mentioned a few times that we are in an arms race with Russia.

Mr. ZUCKERBERG. Yes.

Mr. KINZINGER. If you are giving Russian intelligence service agencies potentially, even on a valid request, access to global data that is not in Russia, is that kind of a disadvantage to us and an advantage to them?

Mr. ZUCKERBERG. Congressman, let me be more precise in my testimony.

Mr. KINZINGER. Sure. Yes, please.

Mr. ZUCKERBERG. I have no specific knowledge of any data that we have ever given to Russia. In general, we will work with valid law enforcement requests in different countries, and we can get back to you on what that might mean with Russia specifically. But I have no knowledge sitting here of any time that we would have given them information.

Mr. KINZINGER. OK. That would with great.

Now, I have got another unique one I want to bring up. So I was just today—and I am not saying this as a woe-is-me, but I think this happens to a lot of people. There have been—my pictures have been stolen and used in fake accounts all around, and in many cases people have been extorted for money. We report it when we can, but we are in a tail chase.

In fact, today I just Googled—or I just put on your website “Andrew Kinzinger,” and he looks a lot like me. But it says he is from London and lives in L.A. And went to Locke High School, which isn't anything like me at all. These accounts pop up a lot, and, again, it is using my pictures but extorting people for money. And we hear about it from people that call and say, “Hey, I was duped,” or whatever.

I know you can't control everything. I mean, you have a huge platform and—but can you talk about maybe some movements into the future to try to prevent that in terms of maybe recognizing somebody's picture and if it is fake?

Mr. ZUCKERBERG. Yes, Congressman. This is an important issue. Fake accounts overall are a big issue because that is how a lot of

the other issues that we see around fake news and foreign election interference are happening as well.

So, long term, the solution here is to build more AI tools that find patterns of people using the services that no real person would do. And we have been able to do that in order to take down tens of thousands of accounts, especially related to election interference leading up to the French election, the German election, and last year the U.S. Alabama Senate State election, Senate election—special election. And that is an area where we should be able to extend that work and develop more AI tools that can do this more broadly.

Mr. KINZINGER. OK. Thank you.

Mr. WALDEN. The gentleman's time has expired.

The Chair recognizes the gentleman from New Mexico, Mr. Luján, for 4 minutes.

Mr. LUJÁN. Thank you, Mr. Chairman.

And I want to pick up where Mr. Kinzinger dropped off here.

Mr. Zuckerberg, Facebook recently announced that a search feature allowed malicious actors to scrape data on virtually all of Facebook's 2 billion users. Yes or no, in 2013, Brandon Copley, the CEO of Giftnix, demonstrated that this feature could easily be used to gather information at scale?

Well, the answer to that question is yes.

Yes or no, this issue of scraping data was again raised in 2015 by a cybersecurity researcher, correct?

Mr. ZUCKERBERG. Congressman, I am not specifically familiar with that. The feature that we identified—I think it was a few weeks ago or a couple weeks ago at this point—was a search feature that allowed people to look up some information that people had publicly shared on their profile, so names, profile pictures, public information.

Mr. LUJÁN. If a may, Mr. Zuckerberg, I will recognize that Facebook did turn this feature off.

My question, and the reason I am asking about 2013 and 2015 is Facebook knew about this in 2013 and 2015, which it didn't turn the feature off until Wednesday of last week, the same feature that Mr. Kinzinger just talked about where this is essentially a tool for these malicious actors to go and steal someone's identity and put the finishing touches on it.

So, again, you know, one of your mentors, Roger McNamee recently said your business is based on trust, and you are losing trust. This is a trust question. Why did it take so long, especially when we are talking about some of the other pieces that we need to get to the bottom of? Your failure to act on this issue has made billions of people potentially vulnerable to identity theft and other types of harmful malicious actors.

So, onto another subject, Facebook has detailed profiles on people who have never signed up for Facebook, yes or no?

Mr. ZUCKERBERG. Congressman, in general, we collect data from people who have not signed up for Facebook for security purposes to prevent the kind of scraping that you were just referring to.

Mr. LUJÁN. So these are called shadow profiles? Is that what they have been referred to by some?

Mr. ZUCKERBERG. Congressman, I am not familiar with that.

Mr. LUJÁN. I will refer to them as shadow profiles for today's hearing.

On average, how many data points does Facebook have on each Facebook user?

Mr. ZUCKERBERG. I do not know off the top of my head.

Mr. LUJÁN. So the average for non-Facebook platforms is 1,500. It has been reported that Facebook has as many as 29,000 data points for an average Facebook user. Do you know how many points of data that Facebook has on the average non-Facebook user?

Mr. ZUCKERBERG. Congressman, I do not off the top of my head, but I can have our team get back to you afterwards.

Mr. LUJÁN. I appreciate that.

It has been admitted by Facebook that you do collect data points on non-average users. So my question is, can someone who does not have a Facebook account opt out of Facebook's involuntary data collection?

Mr. ZUCKERBERG. Congressman, anyone can turn off and opt out of any data collection for ads, whether they use our services or not. But in order to prevent people from scraping public information, which, again, the search feature that you brought up only showed public information, people's names and profiles and things that they had made public, but nonetheless, we don't want people aggregating even public information—

Mr. LUJÁN [continuing]. But so we—

Mr. ZUCKERBERG. So we need to know when someone is trying to repeatedly access our services.

Mr. LUJÁN. If I may, Mr. Zuckerberg, because I am about out of time. It may surprise you that we have not talked about this a lot today. You have said everyone controls their data, but you are collecting data on people that are not even Facebook users, that have never signed a consent, a privacy agreement, and you are collecting their data.

And it may surprise you that, on Facebook's page, when you go to "I don't have a Facebook account and would like to request all my personal data stored by Facebook," it takes you to a form that says, "Go to your Facebook page, and then, on your account settings, you can download your data." So you are directing people that don't even have a Facebook page to have to sign up for a page to erase their data. We have got to fix that.

The last question that I have is, Have you disclosed to this committee or to anyone all information Facebook has uncovered about Russian interference on your platform?

Mr. ZUCKERBERG. Congressman, we are working with the right authorities on that, and I am happy to answer specific questions here as well.

Mr. WALDEN. The gentleman's time has expired.

Mr. LUJÁN. Thank you, Mr. Chairman.

Mr. WALDEN. The Chair now recognizes the gentleman from Virginia, Mr. Griffith, for 4 minutes.

Mr. GRIFFITH. Thank you, Mr. Chairman.

I appreciate you being here.

Let me state upfront that I share the privacy concerns that you have heard from a lot of us, and I appreciate your statements and

willingness to, you know, help us figure out a solution that is good for the American people. So I appreciate that.

Secondly, I have to say that it is my understanding that yesterday Senator Shelley Moore Capito, my friend in my neighboring State of West Virginia, asked you about Facebook's plans with rural broadband, and you agreed to share that information with her at some point in time, get her up to date and up to speed. I was excited to hear that you were excited about that and passionate about it.

My district is very similar to West Virginia as it borders it and we have a lot of rural areas. Can you also agree, yes or no, to update me on that when the information is available?

Mr. ZUCKERBERG. Yes, Congressman. We will certainly follow up with you on this. Part of the mission of connecting everyone around the world means that everyone needs to be able to be on the internet.

And, unfortunately, too much of the internet infrastructure today is too expensive for the current business models of carriers to support a lot of rural communities with the quality of service that they deserve.

So we are building a number of specific technologies from, you know, planes that can beam down internet access to repeaters and mesh networks to make it so that all these communities can be served, and we would be happy to follow up with you on this to—

Mr. GRIFFITH. I appreciate that. And we have got a lot of drone activity going on in our district, whether it is University of Virginia at Wise or Virginia Tech. So we would be happy to help out there too.

Let me switch gears. You talked about trying to ferret out misinformation, and the question becomes who decides what is misinformation. So, when some of my political opponents put on the Facebook that, you know, they think Morgan Griffith is a bum, I think that is misinformation. What say you?

Mr. ZUCKERBERG. Congressman, without weighing in on that specific piece of content, let me outline the way that we approach fighting fake news in general. There are three categories of fake news that we fight: One are basically spammers. They are economic actors like the Macedonian trolls that I think we have all heard about, basically folks who don't have an ideological goal. They are just trying to write the most sensational thing they can in order to get people to click on it so they can make money on ads. It is all economics.

So the way to fight that is we make it so they can't run our ads; they can't make money. We make it so that we can detect what they are doing and show it less in news feeds so they can make less money. When they stop making money, they just go and do something else, because they are economically inclined.

The second category are basically state actors, right, so what we found with Russian interference, and those people are setting up fake accounts. So, for that, we need to build AI systems that can go and identify a number of their fake account networks.

And just last week, we traced back the Russian activity to a specific fake account network that Russia had in Russia to influence Russian culture and other Russian-speaking countries around

them. And we took down a number of their fake accounts and pages, including a news organization that was sanctioned by Russian—by the Russian Government as a Russian state news organization.

So that is a pretty big action, but removing fake accounts is the other way that we can stop the spread of false information.

Mr. GRIFFITH. And I appreciate that. My time is running out. I do want to point this out though as part of that, you know, who is going to decide what is misinformation. We have heard about the Catholic University and the cross. We have heard about a candidate. We have heard about the conservative ladies. A firearms shop, lawful, in my district, had a similar problem. It has also been corrected.

And so I wonder if the industry has thought about—not only are we looking at it, but has the industry thought about doing something like underwriters laboratories, which was set up when electricity was new to determine whether or not the devices were safe?

Have you all thought about doing something like that so it is not Facebook alone but the industry saying, “Wait a minute, this is probably misinformation,” and setting up guidelines that everybody can agree are fair?

Mr. ZUCKERBERG. Yes, Congressman. That is actually the third category that I was going to get to next after economic spammers and state actors with fake accounts. One of the things that we are doing is working with a number of third parties who—so, if people flag things as false news or incorrect, we run them by third-party fact checkers who are all accredited by this Pointer Institute of Journalism. There are firms of all leanings around this who do this work, and that is an important part of the effort.

Mr. WALDEN. The gentleman’s time has expired.

Mr. GRIFFITH. I yield back.

Mr. WALDEN. The Chair now recognizes the gentleman from New York, Mr. Tonko, for 4 minutes.

Mr. TONKO. Thank you.

Mr. Zuckerberg, I want to follow up on a question asked by Mr. McNerney when he talked about visiting websites and the fact that Facebook can track you. And as you visit those websites, you can have that deleted. I am informed that there is not a way to do that, or are you telling us that you are announcing a new policy?

Mr. ZUCKERBERG. Congressman, my understanding is that if we have information from you visiting other places, then you have a way of getting access to that and deleting it and making sure that we don’t store it anymore.

In the specific question that the other Congressman asked, I think it is possible that we just didn’t have the information that he was asking about in the first place, and that is why it wasn’t there.

Mr. TONKO. Well, 3 billion user accounts were breached at Yahoo in 2013; 145 million at eBay in 2014; 143 million at Equifax in 2017; 78 million at Anthem in 2015; 76 million at JPMorgan Chase in 2014. The list goes on and on.

The security of all that private data is gone, likely sold many times over to the highest bidder on the dark web. We live in an

information age. Data breaches and privacy hacks are not a question of if; they are a question of when.

The case with Facebook is slightly different. The 87 million accounts extracted by Cambridge Analytica are just the beginning, with likely dozens of other third parties that have accessed this information. As far as we know, the dam is still broken.

As you have noted, Mr. Zuckerberg, Facebook's business model is based on capitalizing on the private personal information of your users. Data security should be a central pillar of this model.

And with your latest vast breach of privacy and the widespread political manipulation that followed it, the question this committee must ask itself is what role the Federal Government should play in protecting the American people and the democratic institutions that your platform and others like it have put at risk.

In this case, you gave permission to mine the data of some 87 million users based on the deceptive consent of just a fraction of that number. When they found out I was going to be speaking with you today, my constituents asked me to share some of their concerns in person.

How can they protect themselves on your platform? Why should they trust you again with their likes, their loves, their lives? Users trusted Facebook to prioritize user privacy and data security, and that trust has been shattered. I am encouraged that Facebook is committed to making changes, but I am indeed wary that you are only acting now out of concern for your brand and only making changes that should have been made a long time ago.

You have described this as an arms race, but every time we saw what precautions you have or, in most cases, have not taken your company is caught unprepared and ready to issue another apology. I am left wondering again why Congress should trust you again. We will be watching you closely to ensure that Facebook follows through on these commitments.

Many of my constituents have asked about your business model where users are the product. Mary of Halfmoon, in my district, called it infuriating. Andy of Schenectady, New York, asked, why doesn't Facebook pay its users for their incredibly valuable data. Facebook claims that users rightly own and control their data, yet their data keeps being exposed on your platform, and these breaches cause more and more harm each time.

You have said that Facebook was built to empower its users; instead, users are having their information abused with absolutely no recourse. In light of this harm, what liability should Facebook have? When users' data is mishandled, who is responsible, and what recourse do users have? Do you bear that liability?

Mr. ZUCKERBERG. Congressman, I think we are responsible for protecting people's information for sure. But one thing that you said that I want to provide some clarity on—

Mr. TONKO. Do you bear the liability?

Mr. ZUCKERBERG. Well, you said earlier, you referenced that you thought that we were only taking action after this came to light. Actually, we made significant changes to the platform in 2014 that would have made this incident with Cambridge Analytica impossible to happen again today.

I wish we had made those changes a couple of years earlier because this poll app got people to use it back in 2013 and 2014, and if we had made the changes a couple of years earlier, then we would have——

Mr. WALDEN. The gentleman's time has expired.

The Chair recognizes——

Mr. TONKO. Mr. Chairman, if I might ask that other questions that my constituents have be entered by unanimous consent.

Mr. WALDEN. Sure. Without objection, of course.

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

Mr. WALDEN. That goes for all Members.

The Chair recognizes the gentleman from Florida, Mr. Bilirakis, for 4 minutes.

Mr. BILIRAKIS. Thank you. Thank you, Mr. Chairman. I appreciate it.

And thanks for your testimony, Mr. Zuckerberg.

Well, first of all, I wanted to follow up with Mr. McKinley's testimony. This is bad stuff, Mr. Zuckerberg, with regard to the illegal online pharmacies. When are those ads—I mean, when are you going to take those off? I think we need an answer to that. I think we need to get these off as soon as possible.

Can you give us an answer, a clear answer as to when these pharmacies—we have an epidemic here with regard to the opioids. I think we are owed a clear answer, a definitive answer as to when these ads will be offline.

Mr. ZUCKERBERG. Congressman, if people flag those ads for us, we will take them down now.

Mr. BILIRAKIS. Now?

Mr. ZUCKERBERG. Yes.

Mr. BILIRAKIS. By the end of the day?

Mr. ZUCKERBERG. If people flag them for us, we will look at them as quickly as we can.

Mr. BILIRAKIS. Well, you have knowledge now, obviously.

Mr. ZUCKERBERG. Sorry?

Mr. BILIRAKIS. You have knowledge of those ads. Will you begin to take them down today?

Mr. ZUCKERBERG. The ads that are flagged for us we will review and take down if they violate our policies, which I believe the ones that you are talking about——

Mr. BILIRAKIS. They clearly do. If they are illegal, they clearly violate your policy.

Mr. ZUCKERBERG. Which they do. But what I think really needs to happen here is not just us reviewing content that gets flagged for us. We need to be able to build tools that can proactively go out and identify what might be these ads for opioids before people even have to flag them for us to review.

Mr. BILIRAKIS. I agree.

Mr. ZUCKERBERG. And that is going to be a longer-term thing in order to build that solution. So but, today, if someone flags the ads for us, we will take them down.

Mr. BILIRAKIS. Work on those tools as soon as possible, please.

OK. Next question. A constituent of mine in District 12 of Florida, Tampa Bay area, came to me recently with what was a clear violation of your privacy policy. In this case, a third-party organiza-

tion publicly posted personal information about my constituent on his Facebook page.

This included his home address, voting record, degrading photos, and other information. In my opinion, this is cyberbullying. For weeks, my constituent tried reaching out to Facebook on multiple occasions through its report feature, but the offending content remained. It was only when my office got involved that the posts were removed almost immediately for violating Facebook policy.

How does Facebook's self-reporting policy work to prevent misuse, and why did it take an act of Congress, a Member of Congress, to get, again, a clear privacy violation removed from Facebook? If you can answer that question, I would appreciate it, please.

Mr. ZUCKERBERG. Congressman, that clearly sounds like a big issue and something that would violate our policies. I don't know have specific knowledge of that case, but what I imagine happened, given what you just said, is they reported it to us and one of the people who reviews content probably made an enforcement error. And then when you reached out, we probably looked at it again and realized that it violated the policies and took it down.

We have a number of steps that we need to take to improve the accuracy of our enforcement.

Mr. BILIRAKIS. Absolutely.

Mr. ZUCKERBERG. That is a big issue, and we need to get to content faster, and we need to be able to do better at this. I think the same solution to the opioid question that you raised earlier of doing more with automated tools will lead to both faster response times and more accurate enforcement of the policies.

Mr. BILIRAKIS. Can you give us a timeline, as to when will this be done? I mean, this is very critical for—I mean, listen, my family uses Facebook, my friends, my constituents. We all use Facebook. I use Facebook. It is wonderful for our seniors to connect with their relatives.

Mr. WALDEN. The gentleman's time has expired.

Mr. BILIRAKIS. Yes. I am sorry. Can I submit for the record my additional questions?

Mr. WALDEN. Yes, sir.

Mr. BILIRAKIS. Thank you. Thank you so much.

Mr. WALDEN. The Chair recognizes the gentlelady from New York, Ms. Clarke, for 4 minutes.

Ms. CLARKE. I thank you, Mr. Chairman.

And thank you for coming before us, Mr. Zuckerberg, today.

I want to take the opportunity to represent the concerns of the newly formed Tech Accountability Caucus, in which I serve as a co-chair with my colleagues, Representative Robin Kelly, Congressman Emanuel Cleaver, and Congresswoman Bonnie Watson Coleman, but, most importantly, people in our country and around the globe or in vulnerable populations, including those who look just like me.

My first question to you is, as you may be aware, there have been numerous media reports about how more than 3,000 Russian ads were bought on Facebook to incite racial and religious division and chaos in the U.S. during the 2016 election.

Those ads specifically characterized and weaponized African American groups like Black Lives Matter, in which ads suggested



through propaganda or fake news, as people call it these days, that they were a rising threat.

Do you think that the lack of diversity, culturally competent personnel in your C-Suite and throughout your organization, in which your company did not detect or disrupt and investigate these claims, are a problem in this regard?

Mr. ZUCKERBERG. Congresswoman, I agree that we need to work on diversity. In this specific case, I don't think that that was the issue because we were, frankly, slow to identifying the whole Russian misinformation operation and not just that specific example.

Going forward, we are going to address this by verifying the identity of every single advertiser who is running political or issue-oriented ads to make it so that foreign actors or people trying to spoof their identity or say that they are someone that they are not cannot run political ads or run large pages of the type that you are talking about.

Ms. CLARKE. So, whether they were Russian or not, when you have propaganda, how are you addressing that? Because this was extremely harmful during the last election cycle, and it can continue to be so in the upcoming elections and throughout the year, right?

I am concerned that there are not eyes that are culturally competent looking at these things and being able to see how this would impact on civil society. If everyone within the organization is monolithic, then you can miss these things very easily. And we have talked about diversity forever with your organization.

What can you say today when you look at how all of this operates that you can do immediately to make sure that we have the types of viewing or reviewing that can enable us to catch this in its tracks?

Mr. ZUCKERBERG. Congresswoman, we announced a change in how we are going to review ads and big pages so that now, going forward, we are going to verify the identity and location of every advertiser who is running political or issue ads or—and the identities of anyone running—

Ms. CLARKE. We would like you to get back to us with a timeline on that.

Mr. ZUCKERBERG. Oh, that will be in place for these elections.

Ms. CLARKE. OK. Fabulous.

When Mr. Kogan sold the Facebook-based data that he acquired through the quiz app to Cambridge Analytica, did he violate Facebook's policies at the time?

Mr. ZUCKERBERG. Yes, Congresswoman.

Ms. CLARKE. When the Obama campaign collected millions of Facebook users' data through their own app during the 2012 election, did it violate Facebook's policies at the time?

Mr. ZUCKERBERG. No, Congresswoman, it did not.

Ms. CLARKE. I hope you understand that this distinction provides little comfort to those of us concerned about our privacy online.

Regardless of political party, Americans desperately need to be protected. Democrats on this committee have been calling for strong privacy and data security legislation for years. We really can't wait, Mr. Chairman. I yield back.

Thank you, Mr. Zuckerberg.

Mr. WALDEN. The gentlelady's time has expired.  
The Chair recognizes the gentleman from Ohio, Mr. Johnson, for 4 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. Zuckerberg, thanks for joining us today.

Let me add my name to the list of folks that you are going to get back to on the rural broadband internet access question. Please add my name to that list.

Mr. ZUCKERBERG. Of course.

Mr. JOHNSON. I have got a lot of those folks in my district.

You know, you are a real American success story. There is no question that you and Facebook have revolutionized the way Americans—in fact, the world—communicate and interconnect with one another.

I think one of the reasons that you were able to do that is because nowhere other than here in America, where a young man in college can pursue his dreams and ambitions on his own terms without a big Federal Government overregulating them and telling them what they can and cannot do, could you have achieved something like this.

But in the absence of Federal regulations that would reel that in, the only way it works for the betterment of society and people is with a high degree of responsibility and trust. And you have acknowledged that there have been some breakdowns in responsibility.

And I think sometimes—and I am a technology guy. I have two degrees in computer science. I am a software engineer. I am a patent holder. So I know the challenges that you face in terms of managing the technology.

But oftentimes technology folks spend so much time thinking about what they can do and little time thinking about what they should do. And so I want to talk about some of those should-do kinds of things.

You heard earlier about faith-based material that had been taken down, ads that had been taken down. You admitted that it was a mistake. That was in my district, by the way. Franciscan University, a faith-based university, was the one that did that.

How is your content filtered and determined to be appropriate or not appropriate and policy compliant? Is it an algorithm that does it, or is there a team of a gazillion people that sit there and look at each and every add that make that determination?

Mr. ZUCKERBERG. Congressman, it is a combination of both. So, at the end of the day, we have community standards that are written out and try to be very clear about what is acceptable. And we have a large team of people. As I said, by the end of this year, we are going to have more than 20,000 people working on security and content review across the company.

But in order to flag some content quickly, we also build technical systems in order to take things down. So, if we see terrorist content, for example, we will flag that, and we can take that down.

Mr. JOHNSON. What do you do when you find someone or something that has made a mistake? I mean, I have heard you say several times today that you know a mistake has been made. What kind of accountability is there when mistakes are made?

Because every time a mistake like that is made, it is a little bit of a chip away from the trust and the responsibility factors. How do you hold people accountable in Facebook when they make those kind of mistakes of taking stuff down that shouldn't be taken down or leaving stuff up that should not be left up?

Mr. ZUCKERBERG. Congressman, for content reviewers specifically, their performance is going to be measured by whether they do their job accurately.

Mr. JOHNSON. Do you ever fire anybody when you do stuff like that?

Mr. ZUCKERBERG. I am sure we do. As part of the normal course of running a company, you are hiring and firing people all the time to grow your capacity and manage performance.

Mr. JOHNSON. What happened to the person that took down the Franciscan University ad and didn't put it back up until the media started getting involved?

Mr. ZUCKERBERG. Congressman, I am not specifically aware of that case.

Mr. JOHNSON. Can you take that question for me—my time has expired. Can you take that question for me and get me that answer back, please?

Mr. ZUCKERBERG. We will.

Mr. JOHNSON. OK. Thank you very much.

Mr. WALDEN. The gentleman's time has expired.

The Chair recognizes the gentleman from Iowa, Mr. Loeb sack.

Mr. LOEBSACK. Thank you, Mr. Chairman. I want to thank you and the ranking member for holding this hearing today.

And I want to thank Mr. Zuckerberg for being here today as well. Add my name to the rural broadband list as well. I have one-fourth of Iowa, southeast part of Iowa. We definitely need more help on that front. Thank you.

You may recall last year, Mr. Zuckerberg, that you set out to visit every State in the country to meet different people. And one of those places you visited was, in fact, Iowa, my home State of Iowa, and you did visit the district that I probably represent, and you met some of my constituents.

As you began your tour, you said that you believed in connecting the world and giving everyone a voice and that, quote, you wanted, quote, to personally hear more of those voices. I am going to do the same thing in just a second that a number of my colleagues did and just ask you some questions that were submitted to my Facebook page by some of my constituents.

I do want to say at the outset though—and I do ask for unanimous consent to enter all those questions in the record, Mr. Chair.

Mr. WALDEN. Without objection.

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

Mr. LOEBSACK. I think trust has been the issue today. There is no question about it. I think that is what I am hearing from my constituents. That is what we are hearing from our colleagues.

That is really the question: How can we be guaranteed that, for example, when you agree to some things today, that you are going to follow through and that we are going to be able to hold you accountable, and without perhaps constructing too many rules and

regulations? We would like to keep that to a minimum if we possibly can.

But I do understand that you have agreed that we are going to have to have some rules and regulations so that we can protect people's privacy, so that we can protect that use of the consumer data.

So, going forward from there, I have just got a few questions I will probably have an opportunity to get to. The first one goes to the business model issue because you are publicly traded. Is that correct?

Mr. ZUCKERBERG. Yes.

Mr. LOEBSACK. And you are the CEO?

Mr. ZUCKERBERG. Yes.

Mr. LOEBSACK. Right. And so I have got Lauren from Solon who asks, is it possible for Facebook to exist without collecting and selling our data? Is it possible to exist?

Mr. ZUCKERBERG. Congressman, we don't sell people's data. So I think that that is an important thing to clarify upfront. And then, in terms of collecting data, I mean, the whole purpose of the service is so that you can share the things that you want with the people around you and your friends. So—

Mr. LOEBSACK. Is it possible for you to be in business without sharing the data? Because that is what you have done, whether it was selling or not, sharing the data, providing it to Cambridge Analytica and other folks along the way. Is it possible for your business to exist without doing that?

Mr. ZUCKERBERG. Well, Congressman, it would be possible for our business to exist without having a developer platform. It would not be possible for our business or our products or our services or anything that we do to exist without having the opportunity for people to go to Facebook, put in the content that they want to share, and who they want to share it with, and then go do that. That is the core thing that—

Mr. LOEBSACK. Thank you. I appreciate that.

And then Brenda from Muscatine, she has a question, obviously, related to trust as well. And that is, how will changes promised this time be proven to be completed? She would like to know how is that going to happen.

If there are changes, and you said there have been some changes, how can she and those folks in our districts and throughout America, not just Members of Congress, but how can folks in our districts hold you accountable? How do they know that those changes are, in fact, going to happen? That is what that question is about.

Mr. ZUCKERBERG. Congressman, for the developer platform changes that we announced, they are implemented. We are putting those into place. We announced a bunch of specific things. It is on our blog, and I wrote it in my written testimony, and that stuff is happening.

We are also going back and investigating every single app that had access to a large amount of data before we locked down the platform in the past. We will tell people if we find anything that misused their data, and we will tell people when the investigation is complete.

Mr. LOEBSACK. Thank you. And, finally, Chad from Scott County wants to know, who has my data other than Cambridge Analytica?

Mr. ZUCKERBERG. Congressman, part of what I just said is we are going to do an investigation of every single app that had access to a large amount of people's data. If you signed into another app, then that app probably has access to some of your data.

And part of the investigation that we are going to do is to determine whether those app developers did anything improper, shared that data further beyond that. And if we find anything like that, we will tell people that their data was misused.

Mr. WALDEN. The gentleman's time has expired.

Mr. LOEBSACK. Thank you, Mr. Chair.

Mr. WALDEN. The Chair recognizes the gentleman from Missouri, Mr. Long, for 4 minutes.

Mr. LONG. Thank you, Mr. Chairman.

And thank you, Mr. Zuckerberg, for being here today on a voluntarily basis. I want to put that out here. You were not subpoenaed to be here, as Mr. Barton offered up a little bit ago.

You are the only witness at the table today. We have had 10 people at that table, to give you an idea of what kind of hearings we have had in here. Not too long ago, we had 10. And I would say that if we invited everyone that had read your terms of agreement, terms of service, we could probably fit them at that table.

I also would say that I represent 751,000 people, and out of that 751,000 people, the people in my area that are really worked up about this Facebook and about this hearing today would also fit with you there at the table. So I am not getting the outcry from my constituents about what is going on with Cambridge Analytica and this user agreement and everything else. But there are some things that I think you need to be concerned about.

One question I would like to ask before I go into my questioning is, what was FaceMash, and is it still up and running?

Mr. ZUCKERBERG. No, Congressman. FaceMash was a prank website that I launched in college, in my dorm room, before I started Facebook. There was a movie about this, or it said it was about this. It was of unclear truth. And the claim that FaceMash was somehow connected to the development of Facebook, it isn't, it wasn't, and FaceMash—

Mr. LONG. The timing was the same, right? Just coincidental?

Mr. ZUCKERBERG. It was in 2003.

Mr. LONG. OK.

Mr. ZUCKERBERG. And I took it down in—

Mr. LONG. And that is a site where you rate women?

Mr. ZUCKERBERG. And it actually has nothing to do with—

Mr. LONG. You would put up pictures of two women and decide which one was the better, more attractive of the two. Is that right?

Mr. ZUCKERBERG. Congressman, that is an accurate description of the prank website that I made when I was a sophomore in college.

Mr. LONG. OK. But from that beginning, whether it was actually the beginning of Facebook or not, you have come a long way.

Jan Schakowsky, Congresswoman Schakowsky, this morning said, "Self-regulation simply does not work." Mr. Butterfield, Rep-

representative Butterfield, said that you need more African-American inclusion on your board of directors.

If I was you—a little bit of advice. Congress is good at two things: doing nothing and overreacting. So far, we have done nothing on Facebook. Since your inception in that Harvard dorm room those many years ago, we have done nothing on Facebook. We are getting ready to overreact. So just take that as a shot-across-the-bow warning to you.

You have a good outfit there on your front row behind you, very bright folks. You are Harvard-educated. I have a Yale hat that cost me \$160,000. That is as close as I ever got to an Ivy League school.

But I would like to show you right now a little picture here. Do you recognize these folks?

Mr. ZUCKERBERG. I do.

Mr. LONG. Who are they?

Mr. ZUCKERBERG. I believe—is that Diamond and Silk?

Mr. LONG. That is Diamond and Silk, two biological sisters from North Carolina. I might point out they are African American. And their content was deemed by your folks to be unsafe. So, you know, I don't know what type of a picture this is, if it was taken in a police station or what, in a lineup, but apparently they have been deemed unsafe.

Diamond and Silk have a question for you, and that question is: What is unsafe about two black women supporting President Donald J. Trump?

Mr. ZUCKERBERG. Well, Congressman, nothing is unsafe about that. The specifics of this situation I am not as up to speed on as I probably would be if I didn't—

Mr. LONG. Well, you have 20,000 employees, as you said, to check content. And I would suggest, as good as you are with analytics, that those 20,000 people use some analytical research and see how many conservative websites have been pulled down and how many liberal websites.

One of our talk show hosts at home, Nick Reed, this morning on the radio said that if Diamond and Silk were liberal they would be on the late-night talk show circuit, back and forth. They are humorous. They have their opinion, not that you have to agree or that I have to agree. Do agree, don't agree with them, but the fact that they are conservative—and I would just remember—if you don't remember anything else from this hearing here today, remember: We do nothing, and we overreact. And—

Mr. WALDEN. The gentleman's time—

Mr. LONG [continuing]. We are getting ready to overreact.

So I would suggest you go home and review all these other things people have accused you of today, get with your good team there behind you—

Mr. WALDEN. The gentleman's time has expired.

Mr. LONG. You are the guy to fix this. We are not. You need to save your ship.

Thank you.

Mr. WALDEN. The gentleman's time has expired.

Ms. SCHAKOWSKY. Mr. Chairman, since my name was mentioned, can I just respond?

Mr. WALDEN. Well, I tell you, if we could move on, just because we are going to run out of time for Members down-dais to be able to ask their questions.

Ms. SCHAKOWSKY. OK. I consider Billy Long a good friend. Let me just say that I don't think it was a breach of decorum, and I just take issue with his saying that a very modest bill that I have introduced is an overreach. That is all.

Mr. WALDEN. All right.

Mr. LONG. I didn't say it was an overreach. All I said was—I was just letting—

Mr. WALDEN. I now recognize the gentleman from Oregon, Mr. Schrader, for questions for 4 minutes.

Mr. SCHRADER. Ah, thank you, Mr. Chairman. Appreciate that.

Mr. Zuckerberg, again, thank you for being here. Appreciate your good auspices in voluntarily coming before us.

You have testified that you voluntarily took Cambridge Analytica's word that they had deleted information. You found out subsequently that they did not delete that information, have sent in your own forensics team, which I applaud. I just want to make sure and get some questions answered here.

Can you tell us that they were not told—they were told not to destroy any data, misappropriated data, they may find?

Mr. ZUCKERBERG. Congressman, so you are right that in 2015, when we found out that the app developer Aleksandr Kogan had sold data to Cambridge Analytica, we reached out to him at that point, and we demanded that they delete all the data that they had.

They told us at that point that they had done that. And then a month ago we heard a new report that said that they actually hadn't done that.

Mr. SCHRADER. But I am talking about the direction you have given your forensic team. If they find stuff, they are not to delete it at this point in time? Or are they going to go ahead and delete it?

Mr. ZUCKERBERG. The audit team that we are sending in?

Mr. SCHRADER. Right.

Mr. ZUCKERBERG. The first order of business is to understand exactly what happened. And—

Mr. SCHRADER. I am worried about the information being deleted without law enforcement having the opportunity to actually review that.

Will you commit to this committee that neither Facebook nor its agents have removed any information or evidence from Cambridge Analytica's offices?

Mr. ZUCKERBERG. Congressman, I do not believe that we have. And—

Mr. SCHRADER. And how about Mr. Kogan's office, if I may ask?

Mr. ZUCKERBERG. One specific point on this is that our audit of Cambridge Analytica, we have paused that in order to cede to the U.K. Government, which is conducting its own government audit, which, of course—an investigation, which, of course, takes precedence.

Mr. SCHRADER. With all due respect, what I am getting at is, I would like to have the information available for the U.K. or U.S. law enforcement officials, and I did not hear you commit to that.

Will you commit to the committee that Facebook has not destroyed any data records that may be relevant to any Federal, State, or international law enforcement investigation?

Mr. ZUCKERBERG. Congressman, yes. What I am saying is that the U.K. Government is going to complete its investigation before we go in and do our audit. So they will have full access to all the information.

Mr. SCHRADER. So you suspended your audit pending the U.K.'s investigation.

Mr. ZUCKERBERG. Yes. We have paused it pending theirs.

Mr. SCHRADER. OK.

So it is my understanding that you and other Facebook executives have the ability to rescind or delete messages that are on people's websites.

To be clear, I just want to make sure that, if that is indeed the case, that after you have deleted that information, that somehow law enforcement, particularly relevant to this case, would still have access to those messages.

Mr. ZUCKERBERG. Congressman, yes. We have a document retention policy at the company where, for some people, we delete emails after a period of time, but we of course preserve anything that there is a legal hold on.

Mr. SCHRADER. Great. Well, I appreciate that.

While you have testified very clearly that you do not sell information—that is not Facebook's model. You do the advertising and, obviously, have other means of revenue. But it is pretty clear others do sell that information. Doesn't that make you somewhat complicit in what they are doing? You are allowing them to sell the information that they glean from your website?

Mr. ZUCKERBERG. Well, Congressman, I would disagree that we allow it. We actually expressly prohibit any developer that—

Mr. SCHRADER. How do you enforce that? That is my concern. How do you enforce that? Complaint only is what I have heard so far tonight.

Mr. ZUCKERBERG. Yes, Congressman, some of it is in response to reports that we get. And some of it is we do spot checks to make sure that the apps are actually doing what they say they are doing. And, going forward, we are going to increase the number of audits that we do as well.

Mr. SCHRADER. So last question is, it is my understanding based on the testimony here today that, even after I am off of Facebook, that you guys still have the ability to follow my web interactions. Is that correct?

Mr. ZUCKERBERG. Congressman—

Mr. SCHRADER. I have logged out of Facebook. Do you still have the ability to follow my interactions on the web?

Mr. ZUCKERBERG. Congressman, you have control over what we do for ads and the information collection around that. On security, there may be specific things about how you use Facebook even if you are not logged in that we keep track of to make sure that people aren't abusing the system.



Mr. WALDEN. The gentleman's time has expired.

Mr. SCHRADER. I yield back.

Mr. WALDEN. And just for our Members who haven't had a chance to ask questions, we will pause at—well, we will have votes at 1:40. We will continue the hearing after a brief pause. And we will coordinate that.

We will go now to Dr. Bucshon.

Mr. BUCSHON. Thank you, Mr. Chairman.

Thank you, Mr. Zuckerberg, for being here.

There are plenty of anecdotal examples, including from family members of mine, where people will be verbally discussing items, never having actually been on the internet at the time, and then the next time they get on Facebook or other online apps ads for things that they were verbally discussing with each other will show up.

And I know you said in the Senate that Facebook doesn't listen, specifically listen, to what people are saying through their phone, whether that is a Google phone or whether it is Apple or another one.

However, the other day, my mother-in-law and I were discussing her brother, who had been deceased for about 10 years. And later on that evening, on her Facebook site, she had set to music kind of an in-memoriam picture collage that came up on Facebook specifically to her brother. And that happened the other night.

So, if you are not listening to us on the phone, who is? And do you have specific contracts with these companies that will provide data that is being acquired verbally through our phones or now through things like Alexa or other products?

Mr. ZUCKERBERG. Congressman, we are not collecting any information verbally on the microphone, and we don't have contracts with anyone else who is.

The only time that we might use the microphone is when you are recording a video or doing something where you intentionally are trying to record audio. But we don't have anything that is trying to listen to what is going on in the background.

Mr. BUCSHON. OK. Because, I mean, like I said, I mean, you have talked to people that this has happened to. My son, who lives in Chicago, him and his colleagues were talking about a certain type of suit, because they are business guys, and the next day he had a bunch of ads for different suits when he went onto the internet.

So it is pretty obvious to me that someone is listening to the audio on our phones. And I see that as a pretty big issue, and the reason is because—and you may not be, but I see it as a pretty big issue because, for example, if you are in your doctor's office, if you are in your corporate boardroom, your office, or even personal areas of your home, that is potentially an issue.

And I am glad to hear that Facebook isn't listening, but I am skeptical that someone isn't. And I see this as an industry-wide issue that you could potentially help address.

And the final thing I will just ask is, when you have, say, an executive session or whatever of your corporate board and you have decisions to be made, do you allow the people in the room to have their phones on them?

Mr. ZUCKERBERG. Congressman, we do. I don't think we have a policy that says that your phone can't be on.

And, again, I am not familiar with—Facebook doesn't do this, and I am not familiar with other companies that do either.

My understanding is that a lot of these cases that you are talking about are a coincidence, or someone might be talking about something but then they also go to a website or interact with it on Facebook because they were talking about it, and then maybe they will see the ad because of that, which is a much clearer statement of the intent.

Mr. BUCSHON. OK. Because, if that is the case, then—I mean, I know, for convenience, companies have developed things like Alexa, and I don't want to just—and other companies are developing things like that. But it just seems to me that part of the whole point of those products is not just for your own convenience, but when you are verbally talking about things and you are not on the internet, they are able to collect information on the type of activities that you are engaging in.

So I would implore the industry to look into that and make sure that, in addition to physical exploring the internet and collecting data, that data being taken verbally not be allowed.

Thank you.

Mr. WALDEN. The gentleman's time has expired.

The Chair recognizes the gentleman from Massachusetts, Mr. Kennedy, for 4 minutes.

Mr. KENNEDY. Thank you, Mr. Chairman.

Mr. Zuckerberg, thank you for being here. Thank you for your patience over both days of testimony.

You spoke about the framing of your testimony about privacy, security, and democracy. I want to ask you about privacy and democracy, because I think, obviously, those are linked.

You have said over the course of questioning yesterday and today that users own all of their data. So I want to make sure that we drill down on that a little bit, and I think our colleagues have tried.

That includes, I believe, the information that Facebook requires users to make public. So that would be a profile picture, gender, age range, all of which is public-facing information. Is that right?

Mr. ZUCKERBERG. Yes.

Mr. KENNEDY. OK.

So can advertisers, then, understanding that you, Facebook, maintain the data—you are not settling that to anybody else. But advertisers clearly end up having access to that through agreements with you about how they then target ads to me, to you, to any other user.

Can advertisers in any way use nonpublic data, so data that individuals would not think is necessarily public, so that they can target their ads?

Mr. ZUCKERBERG. Congressman, the way this works is, let's say you have a business that is selling skis, OK? And you have on your profile that you are interested in skiing, but let's say you haven't made that public, but you share it with your friends, so broadly.

We don't tell the advertiser that "here is a list of people who like skis." They just say, "OK, we are trying to sell skis. Can you reach

people who like skis?” And then we match that up on our side without sharing any of that information with the advertisers.

Mr. KENNEDY. Understood, you don’t share that. But they get access to that information so that if they know—they want to market skis to me because I like skis.

In the realm of data that is accessible to them, does Facebook include deleted data?

Mr. ZUCKERBERG. Congressman, no.

And I also would push back on the idea that we are giving them access to the data. We allow them to reach people who said that on Facebook, but we are not giving them access to the data.

Mr. KENNEDY. OK. Fair. Fair.

So can advertisers, either directly or indirectly, get access to or use the metadata that Facebook collects in order to more specifically target ads? So that would include—I know you have talked a lot about how Facebook would use access to information for folks that—well, I might be able to opt in or out about your ability to track me to other websites. Is that used by those advertisers, as well?

Mr. ZUCKERBERG. Congressman, I am not sure I understand the question. Can you give me an example of what you mean?

Mr. KENNEDY. So, essentially, the advertisers that are using your platform, do they get access to information that the user doesn’t actually think is either, one, being generated or, two, is public?

Understanding that, yes, if you dive into the details of your platform, users might be able to shut that off. But I think one of the challenges with the trust here is that there is an awful lot of information that is generated that people don’t think they are generating and that advertisers are being able to target because Facebook collects it.

Mr. ZUCKERBERG. Yes. So, Congressman, my understanding is that the targeting options that are available for advertisers are generally things that are based on what people share.

Now, once an advertiser chooses how they want to target something, Facebook also does its own work to help rank and determine which ads are going to be interesting to which people. So we may use metadata or other behaviors of what you have shown that you are interested in and news feed or other places in order to make our systems more relevant to you. But that is a little bit different from giving that as an option to an advertiser, if that makes sense.

Mr. KENNEDY. Right. But then I guess the question, back to—and I only have 20 seconds. I think one of the rubs that you are hearing is I don’t understand how users then own that data. I think that is part of the rub.

Second, you focus a lot of your testimony and the questions on the individual privacy aspects of this, but we haven’t talked about the societal implication of it. And I think, while I applaud some of the reforms that you are putting forward, the underlying issue here is that your platform has become a mix of—

Mr. WALDEN. The gentleman’s time—

Mr. KENNEDY [continuing]. Two seconds—news, entertainment, social media that is up for manipulation. We have seen that with a foreign actor.

If the changes to individual privacy don't seem to be sufficient to address that underlying issue—

Mr. WALDEN. The gentleman's time has expired.

Mr. KENNEDY. I would love your comments on that at the appropriate time. Thank you.

Mr. WALDEN. The Chair recognizes the gentleman from Texas, Mr. Flores, for 4 minutes.

Mr. FLORES. Thank you, Mr. Chairman.

Mr. Zuckerberg, thank you for being here today. I am up here, top row. I am certain that there are other things you would rather be doing.

The activities of Facebook and other technology companies should not surprise us. I mean, we have seen it before. And, again, don't take this critically, but we saw a large oil company become a monopoly back in the late 1800s, early 1900s. We saw a large telecommunications company become a near-monopoly in the sixties, seventies, and eighties.

And just as Facebook, these companies were founded by bright entrepreneurs. Their companies grew. And, eventually, they sometimes became detached from everyday Americans. And what happened is policymakers then had to step in and reestablish the balance between those folks and everyday Americans.

You didn't intend for this to happen. It did happen. And I appreciate that you have apologized for it. And one of the things I appreciate about Facebook, it appears you are proactively trying to address the situation.

Just as we addressed those monopolies in the past, we are faced with that situation today. And this goes beyond Facebook. This has to do with the edge providers. It has to do with social media organizations and also with ISPs.

Back to Facebook in particular, though, we heard examples yesterday during the Senate hearing and also today during this hearing so far about ideological bias among the users of Facebook. In my Texas district, I had a retired schoolteacher whose conservative postings were banned or stopped. The good news is I was able to work with Facebook's personnel and get her reinstated. That said, the Facebook censors still seem to be trying to stop her postings, and anything you can do in that regard to fix that bias will go a long way.

I want to move a different direction, and that is to talk about the future. Congress needs to consider policy responses, as I said earlier. And I want to call this policy response Privacy 2.0 and Fairness 2.0. With respect to fairness, I think the technology companies should be ideologically agnostic regarding their users' public-facing activities. The only exception would be for potentially violent behavior.

My question is on this: Do you agree that Facebook and other technology platforms should be ideologically neutral?

Mr. ZUCKERBERG. Congressman, I agree that we should be a platform for all ideas and that we should focus on that.

Mr. FLORES. Good.

Mr. ZUCKERBERG. I—

Mr. FLORES. I have to—I have limited time.

With respect to privacy, I think that we need to set a baseline. When we talk about a virtual person that each technology user establishes online—their name, address, their online purchases, geolocation data, websites visited, pictures, et cetera—I think that the individual owns the virtual person that they have set up online.

My second question is this: You have said earlier that each user owns their virtual presence. Do you think that this concept should apply to all technology providers, including social media platforms, edge providers, and ISPs?

Mr. ZUCKERBERG. Congressman, yes, in general. I mean, I think that people own their—

Mr. FLORES. Thank you. I am not trying to cut you off. You can provide more information supplementally afterward, if you don't mind.

In this regard, I believe that if Congress enacts privacy standards for technology providers, just as we have for financial institutions, healthcare, employee benefits, et cetera, the policy should state that the data of technology users should be held privately unless they specifically consent to the use of the data by others.

This release should be based upon the absolute transparency as to what data will be used, how it will be processed, where it will be stored, what algorithms will be applied to it, who will have access to it, if it will be sold, and to whom it might be sold.

The disclosure of this information and the associated opt-in actions should be easy to understand and easier for nontechnical users to execute. The days of the long, scrolling, fine-print disclosures with a single checkmark at the bottom should end. In this regard, based on my use of Facebook—

Mr. WALDEN. The gentleman's—

Mr. FLORES [continuing]. I think you have come a long way toward meeting that objective. I think we must move further.

I will have two other questions to submit later. And thank you. You can expand on your responses to my earlier questions later. Thank you.

Mr. WALDEN. The gentleman's time has expired.

The Chair recognizes the gentleman from California for 4 minutes, Mr. Cárdenas.

Mr. CÁRDENAS. Thank you very much. It seems like we have been here forever, don't you think? Well, thank you, Mr. Chairman and Ranking Member, for holding this important hearing.

I am of the opinion that basically we are hearing from one of the leaders, the CEO, of one of the biggest corporations in the world but yet almost entirely in an environment that is unregulated or, for basic terms, that the lanes in which you are supposed to operate in are very wide and broad, unlike other industries.

Yet, at the same time—I have a chart here of the growth of Facebook. Congratulations to you and your shareholders. It shows that in 2009 your net value of the company was less than—or revenue was less than a billion dollars. And then you look all the way over to 2016; it was in excess of \$26 billion. And then in 2017 apparently you were about close to \$40 billion.

Are those numbers relatively accurate about the growth and the phenomenon of Facebook?

Mr. ZUCKERBERG. Congressman, they sound relatively accurate.  
Mr. CÁRDENAS. OK.

Just so you know, it was just brought to my attention—my staff texted me a little while ago—that the CEO of Cambridge Analytica apparently stepped down sometime today. I don't know if anybody of your team there whispered that to you, but my staff just reported that. That is interesting.

The fact that the CEO of Cambridge Analytica stepped down, does that, in and of itself, solve the issue and the controversy around what they did?

Mr. ZUCKERBERG. Congressman, I don't think so.

There are a couple of big issues here. One is what happened specifically with Cambridge Analytica. How were they able to buy data from a developer that people chose to share it with, and how do we make sure that can't happen again?

Mr. CÁRDENAS. But some of that information did originate with Facebook, correct?

Mr. ZUCKERBERG. People had it on Facebook and then chose to share theirs and some of their friends' information with this developer, yes.

Mr. CÁRDENAS. Uh-huh.

Something was brought to my attention most recently, that apparently Facebook does, in fact, actually buy information to add or augment the information that you have on some of your users to build around them, their profile?

Mr. ZUCKERBERG. Congressman, we just recently announced that we were stopping working with data brokers as part of the ad system. It is—

Mr. CÁRDENAS. But you did do that to build your company in the past?

Mr. ZUCKERBERG. It is an industry standard ad practice. And, recently, upon examining all of our systems, we decided that is not a thing that we want to be part of even if everyone else is doing that.

Mr. CÁRDENAS. But you did engage in that as well. And not just everybody else, but Facebook, yourselves, you did engage in that?

Mr. ZUCKERBERG. Yes, until we announced that we were shutting it down. Yes.

Mr. CÁRDENAS. OK.

It is my understanding that when the Guardian decided to report on the Cambridge Analytica consumer data issue, Facebook threatened to sue them if they went forward with their story. Did it happen something like that? Facebook kind of warned them, like, hey, maybe you don't want to do that?

Mr. ZUCKERBERG. Congressman, I don't believe that—I think that there may have been a specific factual inaccuracy that we—

Mr. CÁRDENAS. So, in other words, you checking the Guardian and saying, "You are not going to want to go out with that story because it is not 100 percent factual," that—

Mr. ZUCKERBERG. On that specific point, yes.

Mr. CÁRDENAS. OK.

But, however, they did go through with their story, regardless of the warnings or the threats of Facebook saying that you are not going to want to do that. When they did do that, and only then,

did Facebook actually apologize for that incident, for that 89 million users' information unfortunately ending up in their hands. Isn't that the case?

Mr. ZUCKERBERG. Congressman, you are right that we apologized after they posted the story. They had most of the details of what was right there, and I don't think we objected to that.

Mr. CÁRDENAS. Thank you.

Mr. ZUCKERBERG. There was a specific thing—

Mr. CÁRDENAS. OK, but I only have a few more seconds.

My main point is this: I think it is time you, Facebook, if you truly want to be a leader in all the senses of the word and recognize that you can, in fact, do right by American users of Facebook, and when it comes to information unfortunately getting in the wrong hands, you can be a leader.

Are you committed to actually being a leader in that sense?

Mr. WALDEN. The gentleman's time—

Mr. CÁRDENAS. Can he give a 2-second answer?

Mr. WALDEN. Sure.

Mr. ZUCKERBERG. Congressman, I am definitely committed to taking a broader view of our responsibility. That is what my testimony is about, making sure that we just don't give people tools but make sure that they are used for good.

Mr. CÁRDENAS. Thank you very much.

Thank you, Mr. Chairman.

Mr. WALDEN. And, with that, we will recess for about 5 minutes—10 minutes. We will recess for 10 minutes and then resume the hearing.

[Recess.]

Mr. WALDEN. All right. We are going to reconvene the Energy and Commerce Committee.

And we will go next to the gentlelady from Indiana, Mrs. Brooks, for 4 minutes to resume questioning.

Mrs. BROOKS. Thank you, Mr. Chairman.

And thank you, Mr. Zuckerberg, for being here today. It is so critically important that we hear from you and your company, because we do believe that it is critically important for you to be a leader in these solutions.

One thing that has been talked about just very little but I think is very important and I want to make sure there is appropriate attention on is how the platform of Facebook but even other platforms—and you have mentioned it a little bit—how you help us in this country keep our country safe from terrorists.

I have talked with lots of people who actually continue to remain very concerned about recruitment of their younger family members, and now we are seeing around the globe an enhanced recruitment of women, as well, to join terrorist organizations.

And so I am very, very concerned. I am a former U.S. Attorney. And so, when 9/11 happened, you didn't exist; Facebook didn't exist. But since the evolution after 9/11, we know that Al Shabaab, al-Qaida, ISIS has used social media like we could not even imagine. So could you please talk about that?

And then you talked about the fact that if there is content that is objectionable or is a danger, that people report it to you. But

what if they don't? What if everybody assumes that someone is reporting something to you?

So I need you to help assure us, as well as the American people, what is Facebook's role, leadership role, in helping us fight terrorism and help us stop the recruitment? Because it is still a grave danger around the world.

Mr. ZUCKERBERG. Congresswoman, thanks for the question.

Terrorist content and propaganda has no place in our network, and we have developed a number of tools that have now made it so that 99 percent of the ISIS and al-Qaida content that we take down is identified by these systems and taken down before anyone in our system even flags it for us.

So that is an example of removing harmful content that we are proud of and that I think is a model for other types of harmful content as well.

Mrs. BROOKS. Can I ask, though—and I appreciate that. And I have heard you say 99 percent, and yet I didn't go out and, you know, look for this, but yet, as recently as March 29, ISIS content was discovered on Facebook, which included an execution video—March 29. On April 9, there were five pages, located on April 9, of Hezbollah content and so forth.

And so what is the mechanism that you are using? Is it artificial intelligence? Is it the 20,000 people? What are you using to—because it is not—I appreciate that no system is perfect, but yet this is just within a week.

Mr. ZUCKERBERG. Congresswoman, it is a good question. And it is a combination of technology and people.

We have a counterterrorism team at Facebook which is—

Mrs. BROOKS. How large is it?

Mr. ZUCKERBERG. Two hundred people—just focused on counterterrorism. And there are other content reviewers who are reviewing content that gets flagged to them as well.

So those are folks who are working specifically on that. I think we have capacity in 30 languages that we are working on. And, in addition to that, we have a number of AI tools that we are developing, like the ones that I had mentioned, that can proactively go flag the content.

Mrs. BROOKS. And so you might have those people looking for the content. How are they helping block the recruiting?

Mr. ZUCKERBERG. Yes, so they—

Mrs. BROOKS. Your platform, as well as Twitter and then WhatsApp, is how they begin to communicate, which I understand you own. Is that correct?

Mr. ZUCKERBERG. Yes.

Mrs. BROOKS. So how are we stopping the recruiting and the communications?

Mr. ZUCKERBERG. So we identify what might be the patterns of communication or messaging that they might put out and then design systems that can proactively identify that and flag those for our teams. That way, we can go and take those down.

Mrs. BROOKS. Thank you. My time is up. I thank you, and please continue to work with us and all the governments who are trying to fight terrorism around the world.

Thank you.



Mr. ZUCKERBERG. Thank you. We will.

And, Mr. Chairman, if you don't mind, before we go to the next question, there was something that I wanted to correct in my testimony from earlier—

Mr. WALDEN. Sure.

Mr. ZUCKERBERG [continuing]. When I went back and talked to my team afterwards.

I had said that if—this was in response to a question about whether web logs that we had about a person would be in “download your information.” I had said that they were. And I clarified with my team that, in fact, the web logs are not in “download your information.” We only store them temporarily. And we convert the web logs into a set of ad interests that you might be interested in those ads, and we put that in the “download your information” instead, and you have complete information over that.

So I just wanted to clarify that for the record.

Mr. WALDEN. I appreciate that. Thank you.

We will go now to the gentleman from California, Mr. Ruiz.

Mr. RUIZ. Thank you, Mr. Chairman.

And thank you, Mr. Zuckerberg, for appearing before the committee today.

The fact is, Mr. Zuckerberg, Facebook failed its customers. You have said as much yourself. You have apologized, and we appreciate that. We, as Congress, have a responsibility to figure out what went wrong here and what could be done differently to better protect consumers' private digital data in the future.

So my first question for you, Mr. Zuckerberg, is, why did Facebook not notify the FTC in 2015 when you first discovered this had happened? And was it the legal opinion of your company that you were under no obligation to notify the FTC, even with the 2011 consent order in place?

Mr. ZUCKERBERG. Congressman, in retrospect, it was a mistake, and we should have and I wish we had notified and told people about it then.

Mr. RUIZ. Did you think that—

Mr. ZUCKERBERG. The reason why we didn't—

Mr. RUIZ [continuing]. The rules were kind of lax, that you were sort of debating whether you needed to or something?

Mr. ZUCKERBERG. Yes, Congressman, I don't believe that we necessarily had a legal obligation to do so. I just think that it was probably—

Mr. RUIZ. OK.

Mr. ZUCKERBERG. I think that it was the right thing to have done. The reason we didn't do it at that time—

Mr. RUIZ. No, no. You answered my question.

Would you agree that for Facebook to continue to be successful it needs to continue to have the trust of its users?

Mr. ZUCKERBERG. Absolutely.

Mr. RUIZ. Great.

So does this not, perhaps, strike you as a weakness with the current system, that you are not required to notify the FTC of a potential violation of your own consent decree with them and that you did not have clear guidelines for what you as a company needed to

do in this situation to maintain the public's trust and act in their best interests?

Mr. ZUCKERBERG. Congressman, regardless of what the laws or regulations are that are in place, we take a broader view of our responsibilities around privacy. And I think that we should have notified people because it would have been the right thing to do. And we are committed—

Mr. RUIZ. I am just trying to think of the other CEO who might not have such a broad view and might interpret the different legal requirements maybe differently. So that is why I am asking these questions. I am also taking a broad view, as a Congressman here, to try to fix this problem.

So, from what we have learned over the past 2 days of hearings, it just doesn't seem like the FTC has the necessary tools to do what needs to be done to protect consumer data and consumer privacy, and we can't exclusively rely on companies to self-regulate in the best interest of consumers.

So, Mr. Zuckerberg, would it be helpful if there was an entity clearly tasked with overseeing how consumer data is being collected, shared, and used and which could offer guidelines, at least guidelines, for companies like yours to ensure your business practices are not in violation of the law, something like a digital consumer protection agency?

Mr. ZUCKERBERG. Congressman, I think it is an idea that deserves a lot of consideration. I am not the type of person who thinks that there should be no regulation, especially because the internet is getting to be so important in people's lives around the world, but I think the details on this really matter. And whether it is an agency or a law that is passed or the FTC has certain abilities, I think that that is all something that we should—

Mr. RUIZ. Well, one of the things that we are realizing is that there are a lot of holes in the system, that, you know, you don't have the toolbox to monitor 9 million apps and tens of thousands of data collectors, and there is no specific mechanism for you to collaborate with those that can help you prevent these things from happening.

And so I think that, perhaps, if we started having these discussions about what would have been helpful for you to build your toolbox and for us to build our toolbox so that we can prevent things like Cambridge Analytica, things like identity theft, things like, you know, what we are seeing, what we have heard about today—so, you know, I just want to thank you for your thoughts and testimony.

So it is clear to me that this is the beginning of many, many conversations on the topic, and I look forward to working with you and the committee to better protect consumer privacy.

Mr. ZUCKERBERG. Congressman, we look forward to following up too.

Mr. WALDEN. We will now go to the gentleman from Oklahoma, Mr. Mullin, for 4 minutes.

Mr. MULLIN. Thank you, Mr. Chairman.

And, sir, thank you for being here. I appreciate you using the term "Congressman" and "Congresswoman." My name is Markwayne Mullin, and feel free to use that name.

Sir, I just want to tell you—first of all, I want to commend you on your ability to not just invent something but to see it through its growth. We see a lot of inventors had the ability to do that, but to manage it and to see it through its tremendous growth period takes a lot of talent. And by your showing here today, you handle yourself well, so thank you on that. And you also do that by hiring the right people, so I commend you on doing that also. You hire people, obviously, based on their ability to get the job done.

Real quick, a couple questions I have. And I will give you time to answer it.

Isn't it the consumers' responsibility, to some degree, to control the content to which they release?

Mr. ZUCKERBERG. Congressman, I believe that people should have the ability to choose to share their data how they want, and they need to understand how that is working. But I agree with what you are saying, that people want to have the ability to move their data to another app, and we want to give them the tools to do that.

Mr. MULLIN. Right.

And does the device settings, does it really help you protect what information is released? For instance, there has been a lot of talk about them searching for something, maybe on Google, and then the advertisement pops up on Facebook. Isn't there a setting on most devices to where you can close out the browser without Facebook interacting with that?

Mr. ZUCKERBERG. Yes, Congressman. On most devices, the way the operating system is architected would prevent something that you do in another app, like Google, from being visible to the Facebook app.

Mr. MULLIN. See, I come from the background of believing that everything I do I assume is opened for anybody to take when I am on the internet. I understand that there are privacy concerns, but you are still releasing it to something farther than a pen and pad. So, once I am on the web or I am on an app, then that information is subject to going really anywhere. All I can do is protect it the best I can by my settings.

And so what I am trying to get to is, as an individual, as a user of Facebook, how can someone control keeping the content within the realm that they want to keep it without it being collected?

You say that, you know, you don't sell it. However, you do sell advertisements. As a business owner, I have a demographic that I go after, and I search advertisers that market to that demographic. So you collect information for that purpose, right?

Mr. ZUCKERBERG. Congressman, yes, we collect information to make sure that the ad experience on Facebook can be relevant and valuable to the small businesses and—

Mr. MULLIN. Sure.

Mr. ZUCKERBERG [continuing]. Others who want to reach people.

Mr. MULLIN. Value-based. But if I am a customer or a user of Facebook and I don't want that information to be shared, how do I keep that from happening? Are there settings within the app that I need to go to to block all that?

Mr. ZUCKERBERG. Congressman, yes there is. There is a setting—so if you don't want any data to be collected around advertising, you can turn that off, and then we won't do it.

In general, we offer a lot of settings over every type of information that you might want to share on Facebook and every way that you might interact with the system, from here is the content that you put on your page, to here is who can see your interests, to here is how you might show up in search results if people look for you, to here is how you might be able to sign into developer apps and log in with Facebook, and advertising.

And we try to make the controls as easy to understand as possible. You know, it is a broad service. People use it for a lot of things, so there are a number of controls, but we try to make it as easy as possible and to put those controls in front of people so that they can configure the experience in the way that they want.

Mr. MULLIN. Would that have kept apps from seeking our information?

Mr. WALDEN. The gentleman's time—

Mr. MULLIN. Thank you. I appreciate it.

Thank you, Chairman. I yield back.

Mr. WALDEN. Thank you.

We will recognize now the gentleman from California for 4 minutes.

Mr. PETERS. Thank you, Mr. Chairman.

Thank you, Mr. Zuckerberg, for being with us today. And I know it has been a long day.

I think we can all agree that technology has outpaced the law with respect to the protection of private information. I wonder if you think it would be reasonable for Congress to define the legal duty of privacy that is owed by private companies to their customers with respect to their personal information.

Mr. ZUCKERBERG. Congressman, I think that that makes sense to discuss.

And I agree with the broader point that I think you are making, which is that the internet and technology overall is just becoming a much more important part of all of our lives. The companies and the technology industry are growing—

Mr. PETERS. Right. That is what I mean by it is outpaced.

And I wonder—I also want to take you at your word. I believe you are sincere that you personally place a high value on consumer privacy and that that personal commitment is significant at Facebook today, coming from you, given your position. But I also observe, and you would agree, that the performance on privacy has been inconsistent.

I wonder, you know, myself, whether that is because it is not a bottom-line issue. It appears that the shareholders are interested in maximizing profits. Privacy certainly doesn't drive profits, I don't think, but also may interfere with profits if you have to sacrifice your ad revenues because of privacy concerns.

Would it not be appropriate for us, once we define this duty, to assess financial penalties in a way that would sufficiently send a signal to the shareholders and to your employees, who you must be frustrated with too, that the privacy you are so concerned about is a bottom-line issue at Facebook?

Mr. ZUCKERBERG. Congressman, it is certainly something that we can consider.

Although, one thing that I would push back on is I think it is often characterized as maybe these mistakes happened because there is some conflict between what people want and business interests. I actually don't think that is the case. I think a lot of these hard decisions come down to a lot of different interests between different people.

So, for example, on the one hand, people want the ability to sign into apps and bring some of their information and bring some of their friends' information in order to have a social experience, and, on the other hand, everyone wants their information locked down and completely private. And the question is not a business question as much as which of those equities do you weigh more.

Mr. PETERS. I think part of it is that, but part of it is also what happened with Cambridge Analytica. Some of this data got away from us.

And I would suggest to you that if there were financial consequences to that that made a difference to the business, not people dropping their Facebook accounts, that it would get more attention. And it is not so much a business model choice. I congratulate you on your business model. But it is that these issues aren't getting the bottom-line attention that I think would have made them a priority with respect to Facebook.

Let me just follow up, in my final time, on an exchange you had with Senator Graham yesterday about regulation. And I think the Senator said, do you as a company welcome regulation? You said, if it is the right regulation, then yes. Question: Do you think that the Europeans have it right? And you said, I think they get some things right.

I wanted you to elaborate on what the Europeans got right and what do you think they got wrong.

Mr. ZUCKERBERG. Congressman, well, there are a lot of things that the Europeans do, and I think that—I think GDPR, in general, is going to be a very positive step for the internet. And it codifies—a lot of the things in there are things that we have done for a long time. Some of them are things that I think would be good steps for us to take.

So, for example, the controls that this requires are generally controls, privacy controls, that we have offered around the world for years. Putting the tools in front of people repeatedly, not just having them in settings but putting them in front of people and making sure that people understand what the controls are and that they get affirmative consent, I think is a good thing to do that we have done periodically in the past, but I think it makes sense to do more.

Mr. PETERS. Great. Anything you think they—

Mr. ZUCKERBERG. And I think that is something that the GDPR will require us to do and will be positive.

Mr. PETERS. Anything you think they got wrong?

Mr. ZUCKERBERG. I need to think about that more.

Mr. PETERS. Well, I would appreciate it if you could respond in writing.

I, again, really appreciate you being here.

Thank you, Mr. Chairman.

Mr. WALDEN. Thank you.

We will go now to the gentleman from North Carolina, Mr. Hudson, for 4 minutes.

Mr. HUDSON. Thank you.

Thank you, Mr. Zuckerberg, for being here. This is a long day. You are here voluntarily, and we sure appreciate you being here.

I can say from my own experience, I have hosted two events with Facebook in my district in North Carolina, working with small business and finding ways they can increase their customer base on Facebook, and it has been very beneficial to us. So I thank you for that.

I do want to pivot slightly and frame the discussion in another light for my question. One of the greatest honors I have is I represent the men and women at Fort Bragg, the epicenter of the universe, home of the Airborne, Special Operations. You visited last year.

Mr. ZUCKERBERG. I did.

Mr. HUDSON. Very well-received. So you understand that, due to the sensitive nature of some of the operations these soldiers conduct, that many are discouraged or even prohibited from having a social media presence.

However, there are others who still have profiles. There are some who may have deleted their profiles upon entering military service. Many have family members who have Facebook profiles. And, as we have learned, each one of these users' information may be shared without their consent.

There is no way that Facebook can guarantee the safety of this information on another company's server if they sell this information. If private information can be gathered by apps without explicit consent of the user, they are almost asking to be hacked.

Are you aware of the national security concerns that would come from allowing those who seek to harm our Nation access to information, such as the geographical location of members of our armed services? Is this something that you are looking at?

Mr. ZUCKERBERG. Congressman, I am not specifically aware of that threat, but, in general, there are a number of national security and election-integrity-type issues that we focus on. And we try to take a very broad view of that. And the more input that we can get from the intelligence community, as well, encouraging us to look into specific things, the more effectively we could do that work.

Mr. HUDSON. Great. Well, I would love to follow up with you on that.

It has been said many times here that you refer to Facebook as a platform for all ideas. I know you have heard from many, yesterday and today, about concerns regarding Facebook censorship of content, particularly content that may promote Christian beliefs or conservative political beliefs. I have to bring up Diamond and Silk again, because they are actually from my district, but I think you have addressed these concerns.

But I think it has also become very apparent, and I hope that it has become very apparent to you, that this is a very serious concern. I actually asked on my Facebook page for my constituents to

give me ideas of things they would like me to ask you today, and the most common question was about personal privacy.

So this is something that I think there is an issue—there is an issue that your company, in terms of trust with consumers, that I think you need to deal with. I think you recognize that, based on your testimony today.

But my question to you is, what is the standard that Facebook uses to determine what is offensive or controversial? And how has that standard been applied across Facebook's platform?

Mr. ZUCKERBERG. Congressman, this is an important question. So there are a couple of standards. The strongest one is things that will cause physical harm or threats of physical harm. But then there is a broader standard of hate speech and speech that might make people feel just broadly uncomfortable or unsafe in the community.

Mr. HUDSON. That is probably the most difficult to define, so I guess my question is—

Mr. ZUCKERBERG. It is very—

Mr. HUDSON [continuing]. What standards do you apply to try to determine what is hate speech versus what is just speech you may disagree with?

Mr. ZUCKERBERG. Congressman, that is a very important question and, I think, is one that we struggle with continuously. And the question of what is hate speech versus what is legitimate political speech is, I think, something that we get criticized both from the left and the right on, on what the definitions are that we have.

It is nuanced, and we try to lay this out in our community standards, which are public documents that we can make sure that you and your office get to look through the definitions on this. But this is an area where I think society's sensibilities are also shifting quickly. And it is also very different in different—

Mr. HUDSON. I am just about out of time here. I hate to cut you off, but let me just say that, you know, based on the statistics Mr. Scalise shared and the anecdotes we can provide you, it seems like there is still a challenge when it comes to conservative—

Mr. WALDEN. The gentleman's—

Mr. HUDSON [continuing]. And I hope you will address that.

Mr. ZUCKERBERG. I agree.

Mr. HUDSON. With that, Mr. Chairman, I will stop talking.

Mr. WALDEN. The gentleman's time has expired.

We now go to the gentleman from New York, Mr. Collins, for 4 minutes.

Mr. COLLINS. Thank you, Mr. Chairman.

And I wasn't sure where I would be going with this, but when you are number 48 out of 54 Members, you know, you can do a lot of listening, and I have tried to do that today. And to frame where I am now, I think—first of all, thank you for coming.

And there is a saying, you don't know what you know until you know it. And I really think you have done a great benefit to Facebook, and yourself in particular, as we now have heard, without a doubt, Facebook doesn't sell data. I think the narrative would be: Of course you sell data. And now we know all, across America, you don't sell data. I think that is good for you, a very good clarification.

The other one is that the whole situation we are here is because a third-party app developer, Aleksandr Kogan, didn't follow through on the rules. He was told he can't sell the data, he gathered the data, and then he did what he was not supposed to, and he sold that data. And it is very hard to anticipate a bad actor doing what they are doing until after they have done it. And, clearly, you took actions after 2014.

So one real quick question is, What did change—in, you know, 10 or 20 or 30 seconds, what data was being collected before you locked down the platform, and how did that change to today?

Mr. ZUCKERBERG. Congressman, thank you.

So, before 2014 when we announced the change, someone could sign into an app and share some of their data but also could share some basic information about their friends. And, in 2014, the major change was we said, now you are not going to be able to share any information about your friends.

So, if you and your friend both happen to be playing a game together or on an app listening to music together, then that app could have some information from both of you, because you each had signed in and authorized that app, but, other than that, people wouldn't be able to share information from their friends.

So the basic issue here, where 300,000 people used this poll and the app and then ultimately sold it to Cambridge Analytica and Cambridge Analytica had access to as many as 87 million people's information, wouldn't be possible today. Today, if 300,000 people used an app, the app might have information about 300,000 people.

Mr. COLLINS. Yes. And I think that is a very good clarification as well, because people are wondering, how does 300,000 become 87 million? So that is also something that is good to know.

And in, you know, I guess my last minute, as I have heard the tone here, I have to give you all the credit in the world. I could tell from the tone—we would say “the other side,” sometimes, when we point to our left. But when the Representative from Illinois, to quote her, said, “Who is going to protect us from Facebook,” I mean, that threw me back in my chair. I mean, that was certainly an aggressive—we will use the polite word, “aggressive,”—but, I think, out-of-bounds kind of comment. Just my opinion.

And I have said—I was interviewed by a couple of folks in the break, and I said, you know, as I am listening to you today, I am quite confident that you truly are doing good. You believe in what you are doing. Two-point-two billion people are using your platform. And I sincerely know in my heart that you do believe in keeping all ideas equal, and you may vote a certain way or not, but that doesn't matter. You have 27,000 employees. And I think the fact is that you are operating under a Federal Trade Commission consent decree from 2011. That is a real thing, and it goes for 20 years.

So, when someone said, do we need more regulations, do we need more legislation, I said no. Right now, what we have is Facebook with a CEO whose mind is in the right place, doing the best you can with 27,000 people. But the consent decree does what it does. I mean, there would be significant financial penalties were Facebook to ignore that consent decree.



So I think, as I am hearing this meeting going back and forth, I, for one, think it was beneficial. It is good. I don't think we need more regulations and legislation now. And I want to congratulate you, I think, on doing a good job here today and presenting your case, and we now know things we didn't know beforehand. So thank you again.

Mr. ZUCKERBERG. Thank you.

Mr. WALDEN. OK. Now I think we go next in order to Mr. Walberg, actually, who was here when the gavel dropped. So we will go to Mr. Walberg for 4 minutes.

Mr. WALBERG. Well, thank you, Mr. Chairman. I appreciate that.

And, Mr. Zuckerberg, I appreciate you being here as well. It has been interesting to listen to all of the comments, from both sides of the aisle, to get an idea of the breadth, length, depth, the vastness of our world wide web, social media, and, more specifically, Facebook.

I want to ask three starter questions. I don't think they will take a long answer, but I will let you answer.

Earlier, you indicated that there were bad actors that triggered your platform policy changes in 2014, but you didn't identify who those bad actors were. Who were they?

Mr. ZUCKERBERG. Congressman, I don't, sitting here today, remember a lot of the specifics of early on. But we saw, generally, a bunch of app developers who were asking for permissions to access people's data in ways that weren't connected to the functioning of an app. So they would just say, OK, if you want to log into my app, you would have to share all this content even though the app doesn't actually use that in any reasonable way.

So we looked at that and said, hey, this isn't right, or we should review these apps and make sure that if an app developer is going to ask someone to access certain data that they actually have a reason why they want to get access to it. And, over time, we have made a series of changes that culminated in the major change in 2014 that I referenced before, where ultimately we made it so now a person can sign in but not bring their friends' information with them anymore.

Mr. WALBERG. OK.

Secondly, is there any way—any way—that Facebook can, with any level of certainty, assure Facebook users that every single app on its platform is not misusing their data?

Mr. ZUCKERBERG. Congressman, it would be difficult to ever guarantee that any single—that there are no bad actors.

Mr. WALBERG. OK.

Mr. ZUCKERBERG. Every problem around security is sort of an arms race, right? You have people who are trying to abuse systems, and our responsibility is to make that as hard as possible and to take the necessary precautions for a company of our scale. And I think that the responsibility that we have is growing with our scale, and we need to make sure that we—

Mr. WALBERG. And I think that is an adequate answer. It is a truthful answer.

Can you assure me that ads and content are not being denied based on particular views?

Mr. ZUCKERBERG. Congressman, yes, politically. Although, I think what you—when I hear that, what I hear is, kind of, normal political speech. We certainly are not going to allow ads for terrorist content, for example, so we would be banning those views. But I think that that is something that we would all expect.

Mr. WALBERG. Let me push it here, and I wanted to bring up a screen grab that we had. Again, going back to Representative Upton earlier on, it was his constituent, but was my legislative director for a time. It was his campaign ad that he was going to boost his post, and he was rejected. He was rejected as being—it said here, ad wasn't approved because it doesn't follow advertising policies. "We don't allow ads that contain shocking, disrespectful, or sensational content, including ads that depict violence or threats of violence."

Now, as I read that—and I also know that you have since, or Facebook has since declared, no, that was a mistake, an algorithm problem that went on there. But that is our concern that we have, that it wouldn't be because he had his picture with a veteran, it wouldn't be because he wanted to reduce spending, but pro-life, Second Amendment, those things, and conservative. That causes us some concerns.

So I guess what I am saying here, I believe that we have to have a light touch in regulation. And when I hear some of my friends on the other side of the aisle decry the fact of what is going on now and they were high-fiving what took place in 2012 with President Obama and what he was capable of doing in bringing in and grabbing for use in a political way, I would say the best thing we can do is have these light-of-day hearings, let you self-regulate as much as possible, with a light touch coming from us, but recognizing that, in the end, your Facebook subscribers are—

Mr. WALDEN. The gentleman's time—

Mr. WALBERG [continuing]. Going to tell you what you need to do.

And so thank you for your time.

And thank you for the time you have given me.

Mr. WALDEN. Yep.

I now recognize the gentlelady from California, Mrs. Walters, for 4 minutes.

Mrs. WALTERS. Thank you. Thank you, Mr. Chairman.

And thank you, Mr. Zuckerberg, for being here.

One of my biggest concerns is the misuse of consumer data and what controls users have over their information. You have indicated that Facebook users have granular control over their own content and who can see it.

As you can see on the screen, on the left is a screen shot of the on/off choice for apps, which must be on for users to use apps that require a Facebook login and which allows apps to collect your information.

On the right is a screen shot of what a user sees when they want to change the privacy settings on a post, photo, or other content. Same account, same user. But which control governs, the app platform access or the user's decision as to who they want to see a particular post?

Mr. ZUCKERBERG. Sorry. Could you repeat the—

Mrs. WALTERS. So which app governs, OK, or which control governs, the app platform access or the user's decision as to who they want to see a particular post? So if you look up there on the screen.

Mr. ZUCKERBERG. Yes. Congresswoman, so, when you are using the service, if you share a photo, for example, and you say, "I only want my friends to see it," then in News Feed and Facebook, only your friends are going to see it. If you then go to a website and then you want to sign into that website, that website can ask you and say, "Hey, here are the things that I want to get access to in order for you to use the website." If you sign in after seeing that screen where the website is asking for certain information, then you are also authorizing that website to have access to that information.

If you have turned off the platform completely, which is what the control is that you have on the left, then you wouldn't be able to sign into another website. You would have to go reactivate this before that would even work.

Mrs. WALTERS. OK. Do you think that the average Facebook user understands that is how it works, and how would they find this out?

Mr. ZUCKERBERG. Congresswoman, I think that these—that the settings when you are signing into an app are quite clear in terms of every time you go to sign into an app, you have to go through a whole screen that says: Here is the app; here are your friends who use it; here are the pieces of information that it would like to have access to. You make a decision whether you sign in, yes or no, and until you say, "I want to sign in," nothing gets shared.

Similarly, in terms of sharing content, every single time that you would upload a photo, you have to make a decision. It is right there at the top. It says, "Are you sharing this with your friends or publicly or with some group," and every single time that is quite clear.

So, in those cases, yes, I think that this is quite clear.

Mrs. WALTERS. OK. So these user control options are in different locations. And it seems to me that putting all privacy control options in a single location would be more user-friendly. Why aren't they in the same location?

Mr. ZUCKERBERG. Well, Congresswoman, we typically do two things. We have a settings page that has all of your settings in one place in case you want to go and play around or configure your settings. But the more important thing is putting the settings in line when you are trying to make a decision.

So, if you are going to share a photo now, we think that your setting about who you want to share that photo with should be in line right there. If you are going to sign into an app, we think that the—it should be very clear right in line when you are signing into the app what permissions that app is asking for. So we do both. It is both in one place in settings if you want to go to it, and it is in line in the relevant place.

Mrs. WALTERS. OK. California has been heralded by many on this committee for its privacy initiatives. Given that you and other major tech companies are in California and we are still experiencing privacy issues, how do you square the two?

Mr. ZUCKERBERG. Sorry. Can you repeat that?

Mrs. WALTERS. So, given that you and other major tech companies are in California and we are still experiencing privacy issues, how do you square the two?

Mr. ZUCKERBERG. What was the other piece?

Mrs. WALTERS. California has been heralded by many on this committee for its privacy initiatives.

Mr. ZUCKERBERG. Well, Congresswoman, I think that privacy is not something that you can ever—our understanding of the issues between people and how they interact online only grows over time.

So I think we will figure out what the social norms are and the rules that we want to put in place, and then, 5 years from now, we will come back and we will have learned more things, and either that will just be that social norms have evolved and the company's practices have evolved or we will put rules in place.

But I think that our understanding of this is going to evolve over quite a long time. So I would expect that even if, you know, a State like California is forward leaning, that is not necessarily going to mean that we fully understand everything or have solved all the issues.

Mr. WALDEN. The gentlelady's time has expired.

I recognize the gentlelady from Michigan, Mrs. Dingell, for 4 minutes.

Mrs. DINGELL. Thank you, Mr. Chairman.

Mr. Zuckerberg, thank you for your patience.

I am a daily Facebook user, much to my staff's distress. I do it myself. And because we need a little humor, I am even married to a 91-year-old man that is the king of Twitter. But I know Facebook's value. I have used it for a long time. But with that value also comes obligation.

We have all been sitting here for more than 4 hours. Some things are striking during this conversation. As CEO, you didn't know some key facts. You didn't know about major court cases regarding your privacy policies against your company. You didn't know that the FTC doesn't have fining authority and that Facebook could not have received fines for the 2011 consent order.

You didn't know what a shadow profile was. You didn't know how many apps you need to audit. You did not know how many other firms have been sold data by Dr. Kogan other than Cambridge Analytica and Eunoia Technologies, even though you were asked that question yesterday. And, yes, we were all paying attention yesterday. You don't even know all the kinds of information Facebook is collecting from its own users.

Here is what I do know: You have trackers all over the web. On practically every website you go to, we all see the Facebook like or Facebook share buttons. And with the Facebook pixel, people browsing the internet may not even see that Facebook logo. It doesn't matter whether you have a Facebook account. Through those tools, Facebook is able to collect information from all of us.

So I want to ask you, how many Facebook like buttons are there on non-Facebook web pages?

Mr. ZUCKERBERG. Congresswoman, I don't know the answer to that off the top of my head, but we will get back to you.

Mrs. DINGELL. Is the number over 100 million?

Mr. ZUCKERBERG. I believe we have served the like button on pages more than that, but I don't know the number of pages that have the like button on actively.

Mrs. DINGELL. How many Facebook share buttons are there on non-Facebook web pages?

Mr. ZUCKERBERG. I don't know the answer to that exactly off the top of my head either, but that is something that we can follow up with you on.

Mrs. DINGELL. And we think that is over 100 million likely.

How many chunks of Facebook pixel code are there on non-Facebook web pages?

Mr. ZUCKERBERG. Congresswoman, you are asking some specific stats that I don't know off the top of my head, but we can follow up with you and get back to you on all of these.

Mrs. DINGELL. Can you commit to get back to the committee? The European Union is asking for 72 hours on transparency. Do you think we could get that back in committee in 72 hours?

Mr. ZUCKERBERG. Congresswoman, I will talk to my team, and we will follow up.

Mrs. DINGELL. I know you are still reviewing, but do you know now whether there are other fourth parties that had access to the data from someone other than Dr. Kogan, or is this something we are going to find out in a press release down the road?

I think what worries all of us—and you have heard it today—is it has taken almost 3 years to hear about that. And I am convinced that there are other people out there.

Mr. ZUCKERBERG. Congresswoman, as I have said a number of times, we are now going to investigate every single app that had access to a large amount of people's information in the past before we locked down the platform.

I do imagine that we will find some apps that were either doing something suspicious or misused people's data. If we find them, then we will ban them from the platform, take action to make sure that they delete the data, and make sure that everyone involved is informed.

Mrs. DINGELL. And you make it public quickly, not 3 years?

Mr. ZUCKERBERG. As soon as we find them.

Mrs. DINGELL. So I am going to conclude because my time is almost up, that I worry that when I hear companies value our privacy, that it is meant in monetary terms not in the moral obligation to protect it. Data protection and privacy are like clean air and clean water. There need to be clear rules of the road.

Mr. WALDEN. The gentlelady's time has expired.

The Chair recognizes the gentleman from Pennsylvania, Mr. Costello, for 4 minutes.

Mr. COSTELLO. Thank you, Mr. Chairman.

I would echo Congressman Collins' comments as well.

Mr. ZUCKERBERG, I think that we, as Americans, have a concept of digital privacy rights in privacy that aren't necessarily codified, and we are trying to sift through how do we actually make privacy rights in a way that are intelligible for tech and understandable to the community at large. And so my questions are oriented in that fashion.

First, if you look at GDPR, the EU privacy—the law that is about to take effect, what pieces of that do you feel would be properly placed in American jurisprudence, in other words, right to erasure, right to get our data back, right to rectify? Could you share with us how you see that playing out, not just for you but for the smaller companies, because I do believe you have a sincere interest in seeing small tech companies prosper?

Mr. ZUCKERBERG. Yes, Congressman.

So there are a few parts of GDPR that I think are important and good. One is making sure that people have control over how each piece of information that they share is used. So people should have the ability to know what a company knows about them, to control and have a setting about who can see it, and to be able to delete it whenever they want.

The second set of things is making sure that people actually understand what the tools are that are available, so not just having it in some settings page somewhere but put the tools in front of people so that they can make a decision.

And that both builds trust and makes it so that people's experiences are configured in the way that they want. That is something that we have done a number of times over the years at Facebook, but with GDPR, we will now be doing more and around the whole world.

The third piece is there are some very sensitive technologies that I think are important to enable innovation around, like face recognition, but that you want to make sure that you get special consent for, right.

If we make it too hard for American companies to innovate in areas like facial recognition, then we will lose to Chinese companies and other companies around the world where—that are able to innovate on that. But—

Mr. COSTELLO. Do you feel you should be able to deploy AI for facial recognition for a non-FB user?

Mr. ZUCKERBERG. Congressman, I think that that is a good question, and I think that this is something that probably—that we should—that people should have control over how it is used and that we are going to be rolling out and asking people whether they want us to use it for them around the world as part of this push that is upcoming.

But I think, in general, for sensitive technologies like that, I do think you want a special consent. I think that would be a valuable thing to consider.

Mr. COSTELLO. Right. Two quick ones. Is Facebook, in utilizing that platform, ever a publisher, in your mind?

Mr. ZUCKERBERG. Congressman—

Mr. COSTELLO. You would say you are responsible for content, right?

Mr. ZUCKERBERG. Yes.

Mr. COSTELLO. You said that yesterday. Are you ever a publisher, as the term is legally used?

Mr. ZUCKERBERG. Congressman, I am not familiar with how the term is legally used.

Mr. COSTELLO. Would you ever be legally responsible for the content that is put onto your platform?

Mr. ZUCKERBERG. Well, Congressman, let me put it this way: There is content that we find, specifically in video today—

Mr. COSTELLO. Right.

Mr. ZUCKERBERG. And when we are commissioning a video to be created, I certainly think we have full responsibility—

Mr. COSTELLO. Agree.

Mr. ZUCKERBERG [continuing]. Of owning that content.

Mr. COSTELLO. Which is what, I think, Chairman Walden's question was upfront. Right.

Mr. ZUCKERBERG. But the vast majority of the content on Facebook is not something that we commissioned. For that, I think our responsibility is to make sure that the content on Facebook is not harmful, that people are seeing things that are relevant to them and that encourage interaction and building relationships with the people around them. And that, I think, is the primary responsibility that we have.

Mr. COSTELLO. My big concern—I am running out of time—is someone limits their data to not being used for something that it might potentially be used for that they have no idea what—how it might actually socially benefit.

And I am out of time, but I would like for you to share at a later point in time how the data that you get might be limited by a user and your inability to use that data may actually prevent the kind of innovation that would bring about positive social change in this country? Because I do believe that was the intention and objective of your company, and I do believe you perform it very, very well in a lot of ways.

Thank you. I yield back.

Mr. ZUCKERBERG. Thank you.

Mr. WALDEN. The gentleman yields back.

I go now to the gentleman from Georgia, Mr. Carter, for 4 minutes.

Mr. CARTER. Thank you, Mr. Chairman.

Thank you, Mr. Zuckerberg, for being here. You are almost done. When you get to me, that means you are getting close to the end, so congratulations. Thank you for being here. We do appreciate it.

You know, you wouldn't be here if it wasn't for the privacy, people's information and the privacy and the fact that we had—you had this lapse. You know all about fake news. You know all about foreign intervention. I know you are concerned about that. I want to talk about just a few different subjects, if you will.

And I would like to ask you just some yes-or-no questions. Please excuse my redundancy. I know that some Members have already asked you about some of these subjects, but I would like to ask you, Mr. Zuckerberg, did you know that 91 people die every day because of opioid addiction? Yes or no. Did you know that? 91 people every day?

Mr. ZUCKERBERG. I did not know that specifically, but I know it is a terrible—

Mr. CARTER. Did you know that it is estimated to be between 2.5 million to 11.5 million people in this country right now who are addicted to opioids?

Mr. ZUCKERBERG. Yes.

Mr. CARTER. OK. Did you know that the average age of Americans has decreased for the first time in decades as a result of what people are saying is a result of the opioid epidemic?

Mr. ZUCKERBERG. Yes, especially among certain demographics.

Mr. CARTER. Absolutely.

I ask you this because some of the other Members have mentioned that about the ads for fentanyl and other illicit drugs that are on the internet and where you can buy them and about your responsibility to monitor that and make sure that is not happening.

I had the opportunity this past week to speak at the Prescription Drug Abuse and Heroin Summit in Atlanta that Representative Hal Rogers started some years ago. Also, we had the FDA Commissioner there, and he mentioned the fact that he is going to be meeting with CEOs of internet companies to discuss this problem. I hope that you will be willing to at least have someone there to meet with him so that we can get your help in this. This is extremely important.

Mr. ZUCKERBERG. Congressman, I will make sure that someone is there. This is an important issue.

Mr. CARTER. OK. Let me ask you another question, Mr. Zuckerberg. Did you know that there are conservation groups that have provided evidence to the Securities and Exchange Commission that endangered wildlife goods, in preliminary ivory, is extensively traded on closed groups on Facebook?

Mr. ZUCKERBERG. Congressman, I was not specifically aware of that, but I think we know that there are issues with content like this that we need to do more proactive monitoring for.

Mr. CARTER. All right. Well, let me ask you, did you know that there are some conservation groups that assert that there is so much ivory being sold on Facebook that it is literally contributing to the extinction of the elephant species?

Mr. ZUCKERBERG. Congressman, I had not heard that.

Mr. CARTER. OK. And did you know that the American—or excuse me, the Motion Picture Association of America is having problems with piracy of movies and of their products and that not only is this challenging their profits but their very existence. Did you know that that was a problem?

Mr. ZUCKERBERG. Congressman, I believe that has been an issue for a long time.

Mr. CARTER. It has been. It has been. So you did know that?

Well, the reason I ask you this is that I just want to make sure that I understand you have an understanding of a commitment. Look, you said earlier—it may have been yesterday—that hate speech is difficult to discern. And I get that. And I understand that, and you are absolutely right. But these things are not, and we need your help with this.

Now, I will tell you, there are Members of this body who would like to see the internet monitored as a utility. I am not one of those. I believe that that would be the worst thing we could do. I believe it would stifle innovation.

I don't think you can legislate morality, and I don't want to try to do that. But we need a commitment from you that these things that can be controlled like this, that you will help us and that you will work with law enforcement to help us with this.



Look, you love America. I know that. We all know that. We need your help here. I don't want Congress to have to act. You want to see a mess, you let the Federal Government get into this. You will see a mess, I assure you. Please, we need your help with this, and I just need that commitment. Can I get that commitment?

Mr. ZUCKERBERG. Congressman, yes, we take this very seriously. That is a big part of the reason overall, these content issues, why, by the end of this year, we are going to have more than 20,000 people working on security and content review, and we need to build more tools too. I agree.

Mr. CARTER. Thank you very much.

Mr. WALDEN. The gentleman's time has expired.

The Chair recognizes Mr. Duncan for 4 minutes.

Mr. DUNCAN. Thank you, Mr. Chairman.

Usually I am last, but today I think we have one behind me that came in late. Mr. Zuckerberg—

Mr. WALDEN. Only by 2 minutes did he come in late.

Mr. DUNCAN [continuing]. I want to thank you for all the work you have done, and I want to let you know that I have been on Facebook since 2007 and started as a State legislator, used Facebook to communicate with my constituents, and it has been an invaluable tool for me in communicating. We can actually do in real time multiple issues as we deal with them here in Congress, answer questions. It is almost like a townhall in real time.

I also want to tell you that your staff here at the Governmental Affairs Office, Chris Herndon and others, do a fabulous job in keeping us informed. So I want to thank you for that.

Before this hearing, when we heard about it, we asked our constituents and our friends on Facebook what would they want me to ask you. And the main response was addressing the perceived and, in many instances, confirmed bias and viewpoint discrimination against Christians and conservatives on your platform.

Today, listening to this, I think the two main issues are user privacy and censorship. The Constitution of the United States and the First Amendment says Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof, nor will it abridge the freedom of speech, of the press, the right of people to assemble or address the Congress for redress of grievances—petition Congress for redress of grievances.

I have got a copy of the Constitution I want to give you at the end of this hearing. The reason I say all that, this is maybe a rhetorical question, but why not have a community standard for free speech and free exercise of religion that is simply a mirror of the First Amendment with algorithms that are viewed—that have a viewpoint that is neutral? Why not do that?

Mr. ZUCKERBERG. Well, Congressman, I think that we can all agree that certain content like terrorist propaganda should have no place on our network. And the First Amendment, my understanding of it, is that that kind of speech is allowed in the world. I just don't think that it is the kind of thing that we want to allow to spread on the internet.

So, once you get into that, you are already—you are deciding that you take this value that you care about safety and that we don't want people to be able to spread information that could cause

harm. And I think that that—our general responsibility is to allow the broadest spectrum of free expression as we can, and that is why—

Mr. DUNCAN. And I appreciate that answer. You are right about propaganda and other issues there.

And I believe the Constitution generally applies to Government and says that Congress shall make no law respecting—talks about religion, and then it won't abridge the freedom of speech or the press.

But the standard has been applied to private businesses, whether those are newspapers or other media platform. And I would argue that social media has now become a media platform to be considered in a lot of ways the same as other press media. So I think the First Amendment probably does apply and will apply.

Let me ask you this: What will you do to restore the First Amendment rights of Facebook users and ensure that all users are treated equally, regardless of whether they are conservative, moderate, liberal, or whatnot?

Mr. ZUCKERBERG. Well, Congressman, I think that we make a number of mistakes in content review today that I don't think only focus on one political persuasion. And I think it is unfortunate that, when those happen, people think that we are focused on them. And it happens in different political groups. I mean, we have—

Mr. DUNCAN. But in the essence of time, conservatives are the ones that raise the awareness that their content has been pulled. I don't see the same awareness being raised by liberal organizations, liberal candidates, or liberal policy statements.

And I think you have been made aware of this over the last 2 days. You probably need to go back and make sure that those things are treated equal, and I would appreciate you do that. Again, I appreciate the platform. I appreciate the work you do, and we stand willing and able to help you here in Congress because Facebook is an invaluable part of what we do and how we communicate. So thanks for being here.

Mr. ZUCKERBERG. Thank you.

Mr. DUNCAN. I yield back.

Mr. WALDEN. And for our final 4 minutes of questioning comes from Mr. Cramer of North Dakota, former head of the public utility commission there. We welcome your comments. Go ahead.

Mr. CRAMER. Thank you.

And thanks for being here, Mr. Zuckerberg.

You know, "don't eat the fruit of this tree" is the only regulation that was ever initiated before people started abusing freedom. Since then, millions of regulations, laws, and rules have been created in response to an abuse of freedom. Oftentimes that response is more extreme than the abuse, and that is what I fear could happen based on some of the things I have heard today in response to this.

So this national discussion is very important, first of all, not only for these last 2 days but that it continues, lest we over respond, OK. Now, that said, I think that the consumer and industry, whatever industry it is, your company or others like yours, share that

responsibility. So I appreciate both your patience and your preparation coming in today.

But in response to the questions from a few of my colleagues related to the illegal drug ads, I have to admit that there were times when I was thinking, “His answers aren’t very reassuring to me,” and I am wondering what your answer would be as to how quickly you could take down an illegal drug site if there was a \$1 million per-post per-day regulation fine tied to it.

In other words, give it your best. I mean, don’t wait for somebody to flag it. Look for it. Make it a priority. It is certainly far more dangerous than a couple of conservative Christian women on TV. So, please, be better than this.

Mr. ZUCKERBERG. Congressman, I agree that this is very important, and I miscommunicated if I left the impression that we weren’t proactively going to work on tools to take down this content and we are only going to rely on people to flag it for us.

Right now, I think underway we have efforts to focus not only on ads, which has been most of the majority of the questions, but a lot of people share this stuff in groups too and the free part of the product that aren’t paid, and we need to get that content down too.

I understand how big of an issue this is. Unfortunately, the enforcement isn’t perfect. We do need to make it more proactive, and I am committed to doing that.

Mr. CRAMER. And I don’t expect it to be perfect, but I do expect it to be a higher priority than conservative thought.

Speaking of that, I think in some of your responses to Senator Cruz yesterday and some responses today related to liberal bias, you have sort of implied the fact that while you have these 20,000 enforcement folks, you have implied that Silicon Valley—perhaps this was more yesterday—that Silicon Valley is a very liberal place and so the talent pool perhaps leans left in its bias.

Let me suggest that you look someplace perhaps in the middle of the North American content for some people. Maybe even your next big investment of capital could be in the—someplace like, say, Bismarck, North Dakota, or Williston, where you have visited, where people tend to be pretty commonsense and probably perhaps even more diverse than Facebook in some respects. If the talent pool is a problem, then let’s look for a different talent pool, and maybe we can even have a nice big center someplace.

I want to then close with this, because you testified yesterday—and the opening statement by the ranking member of the committee bothered me in that suddenly there is this great concern that the providers, particularly Facebook, other large edge providers and content providers, should be hyperregulated, when all along we, as Republicans, have been talking about net neutrality. We talked about, earlier this year or last year, when we rolled back the internet service provider privacy stuff that seemed tilted heavily in your favor and against them.

Don’t you think that ubiquitous platforms like Google and Facebook and many others should have the same responsibility to privacy as an internet service provider?

Mr. ZUCKERBERG. Congressman, let me answer that in a second. And before I get to that, on your last point, the content reviewers

who we have are not primarily located in Silicon Valley. So I think that was an important point.

Mr. CRAMER. It is.

Mr. ZUCKERBERG. I do worry about the general bias of people in Silicon Valley, but the majority of the folks doing content review are around the world in different places.

To your question about net neutrality, I think that there is a big difference between internet service providers and platforms on top of them. And the big reason is that—well, I just think about my own experience.

When I was starting Facebook I had one choice of an internet service provider. And if I had to potentially pay extra in order to make it so that people could have Facebook as an option for something that they used, then I am not sure that we would be here today.

Platforms, there are just many more. So it may be true that a lot of people choose to use Facebook. The average American, I think, uses about eight different communication and social network apps to stay connected to people.

It just is clearly correct or true that there are more choices on platforms. So even though they can reach large scale, I think the pressure of just having one or two in a place does require us to think a little bit differently about that.

Mr. CRAMER. I will submit to you that I have fewer choices on the platform—in your type of a platform than I do internet service providers even in rural North Dakota.

With that, thank you, Mr. Chairman.

Mr. WALDEN. I suppose you don't want to hang around for another round of questions. Just kidding.

Mr. Zuckerberg, your staff, several of them just passed out behind you.

You know, on a serious note, as we close, I would welcome your suggestions of other technology CEOs we might benefit from hearing from in the future for a hearing on these issues as we look at net neutrality, as we look at privacy issues. These are all important. They are very controversial. We are fully cognizant of that. We want to get it right. And so we appreciate your comments and testimony today.

There are no other Members that haven't asked you questions, and we are not doing a second round. So, seeing that, I just want to thank you for being here. I know we agreed to be respectful of your time. You have been respectful of our questions, and we appreciate your answers and your candor.

As you know, some of our Members weren't able to ask all the questions they had, so they will probably submit those in writing, and we would like getting answers to those back in a timely manner.

I would also like to include the following documents be submitted into the record by unanimous consent: a letter from American Civil Liberties Union; a letter from NetChoice; a letter from the Vietnam Veterans of America, which I referenced in my opening remarks; a letter from Public Knowledge; a letter and an FTC complaint from the Electronic Privacy Information Center; a letter from the Motion Picture Association of America; a letter from ACT, the App Associa-

tion; a letter from the Committee for Justice; a letter from the Trans Atlantic Consumer Dialogue; and a letter from the civil society groups; and a letter from the National Council of Negro Women.

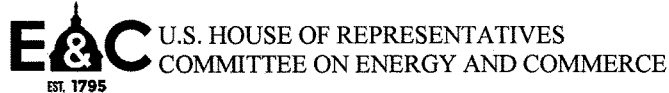
[The information appears at the conclusion of the hearing.]

Mr. WALDEN. Pursuant to committee rules, I remind Members they have 10 business days to submit additional questions for the record. And I ask that the witness submit their responses within 10 business days upon receipt of those questions.

Without objections, our committee is now adjourned.

[Whereupon, at 2:59 p.m., the committee was adjourned.]

[Material submitted for inclusion in the record follows:]



April 9, 2018

TO: Members, Committee on Energy and Commerce

FROM: Committee Majority Staff

RE: Hearing on “Facebook: Transparency and Use of Consumer Data.”

## I. INTRODUCTION

The Committee on Energy and Commerce will hold a hearing on Wednesday, April 11, 2018, at 10:00 a.m. in 2123 Rayburn House Office Building. The hearing is entitled “Facebook: Transparency and Use of Consumer Data.”

## II. WITNESS

- Mark Zuckerberg, Co-Founder, Chairman and CEO, Facebook, Inc.

## III. BACKGROUND

### A. Facebook

Facebook, Inc. (“Facebook”) is a Menlo Park, California based company that operates a variety of social networking and other computerized technology companies. Facebook was started in Cambridge, Massachusetts in 2004 by Mark Zuckerberg, Dustin Moskovitz, and Eduardo Saverin while the trio were students at Harvard University. In 2012, the company publicly listed its shares on the NASDAQ market place. With over 21,000 employees, the company has grown to become the world’s largest social networking website; as of December 31, 2017, the company counts 1.4 billion daily active users, and 2.13 billion monthly active users.<sup>1</sup> The company derives most of its revenue from advertising sales; in 2017, the company generated almost \$40 billion in advertising-derived revenue.<sup>2</sup> It is reported that Facebook and Google receive more than 63 percent of total U.S. digital advertising spending.<sup>3</sup> The company has acquired several other enterprises since its founding, including Instagram, WhatsApp, Masquerade, and Oculus. The company also operates Facebook Payments.<sup>4</sup> Facebook is one of the largest and most successful companies in the world as measured by market capitalization.<sup>5</sup>

<sup>1</sup> “Company Info,” Facebook Newsroom, <https://newsroom.fb.com/company-info/>

<sup>2</sup> “Facebook Reports Fourth Quarter and Full Year 2017 Results,” Facebook Investor Relations, <https://investor.fb.com/investor-news/press-release-details/2018/Facebook-Reports-Fourth-Quarter-and-Full-Year-2017-Results/default.aspx>

<sup>3</sup> “Google and Facebook Tighten Grip on US Digital Ad Market,” emarketer.com (September 21, 2017), <https://www.emarketer.com/Article/Google-Facebook-Tighten-Grip-on-US-Digital-Ad-Market/1016494>

<sup>4</sup> “The Facebook Companies,” Facebook, <https://www.facebook.com/help/111814505650678>

<sup>5</sup> For instance, according to Forbes magazine’s “List of the World’s Biggest Companies,” Facebook was the sixth largest company in the world at the end of 2017. See [https://www.forbes.com/global2000/list/#header:marketValue\\_sortreverse:true](https://www.forbes.com/global2000/list/#header:marketValue_sortreverse:true)

**B. Evolution of the Facebook Platform**

**News Feed and Mini-Feed.** In 2006, Facebook debuted the “news feed,” a curated feed showing what a user’s “Friends” were posting and discussing.<sup>6</sup> The purpose of the feature was to provide users with a centralized destination to minimize the need for a user to browse through every “Friend” profile.<sup>7</sup> However, the feature generated concerns leading to approximately one million Facebook users joining “Facebook News Feed protest groups,” which argued that the new feature was too intrusive.<sup>8</sup> In response, Facebook announced additional privacy controls for the news feed and mini-feed that allowed users to “control... who sees what information.”<sup>9</sup> Additionally, Facebook developed a “privacy page” that gave users “granular control of how information is integrated into” the news feed and mini-feed.<sup>10</sup>

**The Beacon Feature.** In 2007, Facebook launched the Beacon online ad system that would “report back to Facebook on members’ activities on third-party sites that participate in Beacon even if the users are logged off from Facebook and have declined having their activities broadcast to their Facebook friends.”<sup>11</sup> Initially, users were not informed that data on their activities at third-party sites was flowing back to Facebook and users were not given the option to block that information from being transmitted to Facebook. In response to objections, the company changed Beacon “to be an opt-in system” and gave users a “privacy control to turn off Beacon completely.”<sup>12</sup>

**Developer Platform and Privacy Updates.** On May 24, 2007, Facebook launched a Facebook Platform for developers to “build the next-generation of applications with deep integration into Facebook, distribution across its ‘social graph’ and an opportunity to build new businesses.”<sup>13</sup> On November 6, 2007, Facebook introduced Facebook Ads, an “ad system for businesses to connect with users and target advertising to the exact audience they want.”<sup>14</sup> Further, on July 23, 2008, Facebook introduced advancements to Facebook Platform calling on “its more than 400,000 developers to connect their Websites with Facebook through Facebook Connect.”<sup>15</sup> Facebook Connect created a “developer sandbox” whereby users could “bring their Facebook account information, friends and privacy to any third party website, desktop application or device.”<sup>16</sup>

<sup>6</sup> <https://www.nbcnews.com/tech/social-media/can-you-even-remember-how-you-coped-facebook-s-news-n641676>

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> <https://newsroom.fb.com/news/2006/09/facebook-launches-additional-privacy-controls-for-news-feed-and-mini-feed/>

<sup>10</sup> *Id.*

<sup>11</sup> <https://www.pcworld.com/article/140182/article.html>

<sup>12</sup> *Id.*

<sup>13</sup> <https://newsroom.fb.com/news/2007/05/facebook-unveils-platform-for-developers-of-social-applications/>

<sup>14</sup> <https://newsroom.fb.com/news/2007/11/facebook-unveils-facebook-ads/>

<sup>15</sup> <https://newsroom.fb.com/news/2008/07/facebook-expands-power-of-platform-across-the-web-and-around-the-world/>

<sup>16</sup> *Id.*

Majority Memorandum for April 11, 2018, Full Committee Hearing  
Page 3

On May 26, 2010, Facebook responded to privacy concerns by announcing it would “introduce simpler and more powerful controls for sharing personal information.” Specifically, Facebook committed to offering “easier opt outs” whereby users could “completely turn off Platform applications and websites, so that [users’] information [was] not shared with applications, even information available to everyone.”<sup>17</sup> Additionally, Facebook highlighted “new controls users have over information shared with applications and websites on Facebook Platform” that were intended to require applications to obtain specific approval before gaining access to any personal information that a user has not made available to “Everyone.”<sup>18</sup>

On November 13, 2014, Facebook updated their terms and policies and introduced “Privacy Basics,” which gave users tips and a “how-to guide for taking charge” of the Facebook experience.<sup>19</sup> The new feature offered interactive guides designed to answer the most commonly asked questions about how users can control information on Facebook.<sup>20</sup>

On January 26, 2017, Facebook introduced a new version of “Privacy Basics” with a stated goal of making it easier for people to find tools for controlling their information.<sup>21</sup> According to the company, the tool was designed based on users’ most frequently asked questions about privacy and security.<sup>22</sup> Using the tools purportedly provided an easier way for allowing a user to control the user’s account, finding out who can see a user’s post, and seeing what a user’s account looks like to others.<sup>23</sup> The exact number of apps accessible via the Facebook platform is constantly changing; reports say the number exceeds nine million.<sup>24</sup>

After public reports of the use of Facebook data by the political strategy firm Cambridge Analytica the company has announced further privacy changes; these are discussed below.

### C. Issues

**FTC Consent Order.** On November 29, 2011, the Federal Trade Commission (FTC) announced that Facebook and the agency had reached an agreement on a consent order relating to the FTC’s charges that the company had “deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public.”<sup>25</sup> According to the FTC’s Complaint (Complaint), the company had allegedly failed to disclose to Facebook users that “a user’s choice to restrict profile information to ‘Only Friends’

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

<sup>19</sup> <https://newsroom.fb.com/news/2014/11/updates-our-terms-and-policies-helping-you-understand-how-facebook-works-and-how-to-control-your-information/>

<sup>20</sup> *Id.*

<sup>21</sup> <https://newsroom.fb.com/news/2017/01/introducing-the-new-privacy-basics/>

<sup>22</sup> *Id.*

<sup>23</sup> *Id.*

<sup>24</sup> See, e.g., Josh Constantine, *10 years of hope and hard lessons on the Facebook Platform*, Techcrunch.com (April 17, 2017), <https://techcrunch.com/2017/04/17/bizarre-dev-triangle/>; Brittany Darwell, *Facebook platform supports more than 42 million pages and 9 million apps*, Adweek (April 27, 2012) <http://www.adweek.com/digital/facebook-platform-supports-more-than-42-million-pages-and-9-million-apps/>

<sup>25</sup> Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, FTC.gov (November 29, 2011), <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>



Majority Memorandum for April 11, 2018, Full Committee Hearing  
Page 4

or ‘Friends of Friends’ would be ineffective as to certain third parties;” that the company’s “Privacy Wizard” tool for controlling access to user information “did not disclose adequately that users no longer could restrict access to their newly-designated (publicly available information) via their Profile Privacy Settings, Friends’ App Settings, or Search Privacy Settings, or that their existing choices to restrict access to such information via these settings would be overridden;” and that, after making changes to its privacy policy, Facebook “failed to disclose, or failed to disclose adequately, that the December Privacy Changes overrode existing user privacy settings that restricted access to a user’s Name, Profile Picture, Gender, Friend List, Pages, or Networks.”<sup>26</sup>

In response to the Complaint, Facebook and the FTC entered into a Consent Agreement whereby Facebook agreed that it will not “misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information,” including “the extent to which [Facebook] makes or has made covered information accessible to third parties;” that prior to sharing of a user’s nonpublic information, the company will “obtain the user’s affirmative express consent;” and the company would “establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information,” among other stipulations.<sup>27</sup>

**2012 Election.** In 2012, the Obama for America presidential election campaign worked with the company to allow users to sign into the campaign’s website via Facebook.<sup>28</sup> According to accounts at the time, the Facebook application gave the campaign access to both those that signed into the campaign, as well as the “Friends” of such persons—“the more than 1 million Obama backers who signed up for the app gave the campaign permission to look at their Facebook friend lists.”<sup>29</sup> This gave the Obama for America campaign access to “hidden voters” for which they otherwise lacked contact information.<sup>30</sup> Carol Davidsen, Director of Integration of Media Analytics for Obama for America, via Twitter, stated that “Facebook was surprised we were able to suck out the whole social graph, but they didn’t stop us once they realized that was what we were doing.”<sup>31</sup> This in turn allegedly allowed one political party to download and retain individual user data which was not provided to other political organizations.<sup>32</sup>

<sup>26</sup> United States Federal Trade Commission, *In the Matter of Facebook, Inc.*, Complaint, <https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf>

<sup>27</sup> United States Federal Trade Commission, *In the Matter of Facebook, Inc.*, Agreement Containing Consent Order, <https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf>

<sup>28</sup> Kaleve Leetaru, *Why Are We Only Now Talking About Facebook And Elections?*, Forbes.com (March 19, 2018), <https://www.forbes.com/sites/kalevleetaru/2018/03/19/why-are-we-only-now-talking-about-facebook-and-elections/#32e92afb4838>

<sup>29</sup> Michael Scherer, *Friended: How the Obama Campaign Connected with Young Voters*, Time Magazine (Nov. 20, 2012) <http://swampland.time.com/2012/11/20/friended-how-the-obama-campaign-connected-with-young-voters/>

<sup>30</sup> *Id.*

<sup>31</sup> Carol Davidsen via Twitter, (March 18, 2018), <https://twitter.com/cld276/status/975564499297226752>

<sup>32</sup> “Where this gets complicated is, that freaked Facebook out, right? So they shut off the feature. . . (w)ell, the Republicans never built an app to do that. So the data is out there, you can’t take it back, right? So Democrats have this information”- Carol Davidsen, as reported by Jason Howerton, *Ex-Obama Campaign Director: It’s ‘Unfair’ Facebook Let Us ‘Ingest Entire Social Network of US,’* Independent Journal Review (IJR), (March 19, 2018), <https://ijr.com/2018/03/1077208-former-obama-campaign-facebook-data/>

**2016 Election.** In addition to concerns regarding false news stories and fictitious user accounts,<sup>33</sup> concerns have arisen regarding the use of Facebook user data for campaign purposes in the 2016 presidential campaign. According to multiple reports, in 2014, researchers at Cambridge University's Psychometrics Center developed an app that acquired Facebook user data, as well as the data of "Friends" of such users on the social network.<sup>34</sup> Cambridge Analytica, a political consulting firm, allegedly requested the University's assistance in obtaining such data. After Cambridge University refused, the company then approached Mr. Aleksandr Kogan, a professor of psychology at the institution, for help. Mr. Kogan agreed and developed his own app under the auspices of his company Global Science Research (GSR). This application, called "thisisyourdigitallife," similarly harvested the data of users of the social network as well as that of their connections, or "Friends," on the service.<sup>35</sup>

According to reports, over 300,000 users consented to allowing their data to be harvested in exchange for using the "thisisyourdigitallife" app. Consistent with Facebook's policies at the time, use of the app gave Mr. Kogan and Cambridge Analytica access to the data of over 87 million other, non-consenting Facebook users. Cambridge Analytica then used this information to develop and market political messaging services.<sup>36</sup>

According to Facebook, Mr. Kogan's initial access to user data was acquired "in a legitimate way and through the proper channels."<sup>37</sup> However, by subsequently passing on Facebook user data to a third party, the company alleges that Mr. Kogan violated Facebook "platform policies."<sup>38</sup> Additionally, the company received reports that not all Facebook user data had been deleted, as allegedly certified by Mr. Kogan and Strategic Communication Laboratories (SCL)/Cambridge Analytica to Facebook in 2015. In response the company announced it had suspended the parties from Facebook.<sup>39</sup>

Subsequent to the widespread reporting around the incident, Facebook announced several measures it will be implementing to "prevent future abuse."<sup>40</sup> These include investigating apps that had access to large amounts of user data prior to 2014, and auditing any such apps that evince "suspicious activity;" further restricting access for app developers by, among other things, requiring them to sign a contract before asking users for access to posts or other private data; and

<sup>33</sup> For background, see Open Hearing: Social Media Influence in the 2016 U.S. Elections, Senate Select Committee on Intelligence (November 1, 2017) <https://www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections>

<sup>34</sup> See, e.g., See Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, New York Times, (March 19, 2018). <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>

<sup>35</sup> *Id.*

<sup>36</sup> David Pierson, *Facebook says user data of 87 million was shared with Cambridge Analytica*, Los Angeles Times (April 4, 2018), <http://www.latimes.com/business/technology/la-fi-tn-facebook-zuckerberg-20180404-story.html>

<sup>37</sup> Paul Grewal, *Suspending Cambridge Analytica and SCL Group from Facebook*, Facebook Newsroom, (March 16, 2018), <https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/>

<sup>38</sup> *Id.*

<sup>39</sup> *Id.*

<sup>40</sup> *Cracking Down on Future Abuse*, Facebook Newsroom (March 21, 2018) <https://newsroom.fb.com/news/2018/03/cracking-down-on-platform-abuse/>

Majority Memorandum for April 11, 2018, Full Committee Hearing  
Page 6

creating a tool that allows users to more readily see which apps have access to a user's data, and how to limit such access.

#### **D. FTC Action**

On March 26, 2018, the FTC announced that it was opening a non-public investigation into the privacy practices of Facebook. In a press release, the Acting Director of the Commission's Bureau of Consumer Protection stated that "the FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook."<sup>41</sup> If the FTC finds that a party to a previous consent order has violated the terms of that order, it may impose various penalties including fines of up to \$41,484 per day, per violation.<sup>42</sup> The Commission can also seek to modify the existing consent order with additional terms and obligations.

#### **IV. ISSUES**

The following issues may be examined at the hearing:

- Did Facebook allow the harvesting and sale of user data without their consent?
- Did Facebook violate its own policies with respect to the sharing of user data?
- How have Facebook's policies regarding consumer privacy changed since the launch of the Facebook platform?
- What changes has Facebook made or plan to make regarding its use of user information and how that information is made available to third parties?

#### **V. STAFF CONTACTS**

If you have any questions regarding this hearing, please contact Melissa Froelich, Gregory Zerzan, or Bijan Koohmaraie of the Committee staff at (202) 225-2927.

---

<sup>41</sup> Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices, FTC.gov (March 26, 2018) <https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection>

<sup>42</sup> 15 U.S.C. § 45(l)

## Friended: How the Obama Campaign Connected with Young Voters

Social networks are transforming the way campaigns are conducted.

By [Michael Scherer @michaelscherer](#) Nov. 20, 2012

<http://swampland.time.com/2012/11/20/friended-how-the-obama-campaign-connected-with-young-voters/>

In the final weeks before Election Day, a scary statistic emerged from the databases at [Barack Obama's Chicago](#) headquarters: half the campaign's targeted swing-state voters under age 29 had no listed phone number. They lived in the cellular shadows, effectively immune to traditional get-out-the-vote efforts.

For a campaign dependent on a big youth turnout, this could have been a crisis. But the Obama team had a solution in place: a [Facebook](#) application that will transform the way campaigns are conducted in the future. For supporters, the app appeared to be just another way to digitally connect to the campaign. But to the Windy City number crunchers, it was a game changer. "I think this will wind up being the most groundbreaking piece of technology developed for this campaign," says Teddy Goff, the Obama campaign's digital director.

That's because the more than 1 million Obama backers who signed up for the app gave the campaign permission to look at their Facebook friend lists. In an instant, the campaign had a way to see the hidden young voters. Roughly 85% of those without a listed phone number could be found in the uploaded friend lists. What's more, Facebook offered an ideal way to reach them. "People don't trust campaigns. They don't even trust media organizations," says Goff. "Who do they trust? Their friends."

The campaign called this effort targeted sharing. And in those final weeks of the campaign, the team blitzed the supporters who had signed up for the app with requests to share specific online content with specific friends simply by clicking a button. More than 600,000 supporters followed through with more than 5 million contacts, asking their friends to register to vote, give money, vote or look at a video designed to change their mind. A geek squad in Chicago created models from vast data sets to find the best approaches for each potential voter. "We are not just sending you a banner ad," explains Dan Wagner, the Obama campaign's 29-year-old head of analytics, who helped oversee the project. "We are giving you relevant information from your friends."

Early tests of the system found statistically significant changes in voter behavior. People whose friends sent them requests to register to vote and to vote early, for example, were more likely to do so than similar potential voters who were not contacted. That confirmed a trend already noted in political-science literature: online social networks have the power to change voting behavior. A study of 61 million people on Facebook during the 2010 midterms found that people who saw photos of their friends voting on Election Day were more likely to cast a ballot themselves. "It is much more effective to stimulate these real-world ties," says James Fowler, a professor at the University of California at San Diego, who co-authored the study.

Campaign pros have known this for years. A phone call or knock on the door from someone who lives in your neighborhood is far more effective than appeals from out-of-state volunteers or robo-calls. Before social networks like Facebook, however, connecting a supportive friend to a would-be voter was a challenge. E-mail, for instance, connects one person to a campaign. Facebook can connect the campaign, through one person, to 500 or more friends.

Because it took more than a year to build the system, it was deployed only in the campaign's homestretch. The Romney team used a far less sophisticated version of the technology. Political strategists on both sides say that in the future they intend to get the system working sooner in primaries in key states and with more buy-in from supporters, who will have a greater understanding of their role in the process. "Campaigns are trying to engineer what the new door knock is going to look like and what the next phone call is going to look like," says Patrick Ruffini, a Republican digital strategist who worked on George W. Bush's 2004 campaign. "We are starting to see."

And the technology is moving fast. In 2008, Twitter was a sideshow and Facebook had about one-sixth its current reach in the U.S. By 2016, this sort of campaign-driven sharing over social networks is almost certain to be the norm. Tell your friends.

## We Already Know How to Protect Ourselves From Facebook



By **Zeynep Tufekci**

April 9, 2018

<https://www.nytimes.com/2018/04/09/opinion/zuckerberg-testify-congress.html>

This week, Facebook's chief executive, Mark Zuckerberg, is scheduled to testify before two congressional committees amid the growing outcry over the company's data collection practices. Because I have been analyzing the potential negative effects of Facebook on politics for a long time, I am fielding a lot of inquiries about what legislators should ask Mr. Zuckerberg.

Here's my answer: Nothing. We already know most everything we need for legislators to pass laws that would protect us from what Facebook has unleashed.

The sight of lawmakers yelling at Mr. Zuckerberg might feel cathartic, but the danger of a public spectacle is that it will look like progress but amount to nothing: a few apologies from Mr. Zuckerberg, some earnest-sounding promises to do better, followed by a couple of superficial changes to Facebook that fail to address the underlying structural problems.

This has been Facebook's public relations strategy for years. After each scandal, it expresses regrets, announces a few cosmetic fixes and then works like mad to scuttle any legislation that might have a favorable impact on the core problem: how our data is harvested, used and profited from. It would be a shame if we went through that again.

In addition to apologizing, Mr. Zuckerberg will no doubt promise more transparency. Don't get me wrong: I'm all for transparency. But while transparency can help us diagnose problems in the online economy, it alone doesn't fix them.

Mr. Zuckerberg is also likely to promise to lock down all the data Facebook has collected on billions of people. That sounds like a good idea, but it is mostly irrelevant now; the data is already compromised.

More important, it is in Facebook's financial interest to lock down its stores of data. After all, the company's product, which it sells to advertisers and other interested parties, is microtargeted access to *us* and our attention. The extensive data it collects on billions of people is its means of executing that business. It does not want to give that resource away.

So why did it give away people's data in the past? In part because it is a reckless company ("Move fast and break things" used to be a company motto of sorts). And in part because the data — a tantalizing resource for programmers — could be used to lure developers to make games, quizzes and other apps for Facebook that would keep users coming back to the site.

But that phase of the company's development is over. Because Facebook does not sell our data directly (or even want to), extracting promises from Mr. Zuckerberg that it not do so would be worse than a toothless remedy. It would only serve Facebook's business model.

What would a genuine legislative remedy look like? First, personalized data collection would be allowed only through opt-in mechanisms that were clear, concise and transparent. There would be no more endless pages of legalese that nobody reads or can easily understand. The same would be true of any individualized targeting of users by companies or political campaigns — it should be clear, transparent and truly consensual.

Second, people would have access, if requested, to all the data a company has collected on them — including all forms of computational inference (how the company uses your data to make guesses about your tastes and

preferences, your personal and medical history, your political allegiances and so forth).

Third, the use of any data collected would be limited to specifically enumerated purposes, for a designed period of time — and then would expire. The current model of harvesting all data, with virtually no limit on how it is used and for how long, must stop.

Fourth, the aggregate use of data should be regulated. Merely saying that individuals own their data isn't enough: Companies can and will persuade people to part with their data in ways that may seem to make sense at the individual level but that work at the aggregate level to create public harms. For example, collecting health information from individuals in return for a small compensation might seem beneficial to both parties — but a company that holds health information on a billion people can end up posing a threat to individuals in ways they could not have foreseen.

Facebook may complain that these changes to data collection and use would destroy the company. But while these changes would certainly challenge the business model of many players in the digital economy, giant companies like Facebook would be in the best position to adapt and forge ahead.

If anything, we should all be thinking of ways to reintroduce competition into the digital economy. Imagine, for example, requiring that any personal data you consent to share be offered back to you in an “interoperable” format, so that you could choose to work with companies you thought would provide you better service, rather than being locked in to working with one of only a few.

Right now, Silicon Valley is stuck in a (very profitable) rut. To force it to change would not only make us safer but also foster innovation.

That would be a better, more satisfying outcome than any dramatic “Have you no sense of decency, sir?” moment that a congressional hearing might produce.

Zeynep Tufekci ([@zeynep](#)) is an associate professor at the School of Information and Library Science at the University of North Carolina, the



author of “Twitter and Tear Gas: The Power and Fragility of Networked Protest” and a contributing opinion writer.

*Follow The New York Times Opinion section on [Facebook](#) and [Twitter](#) (@NYTopinion), and sign up for the [Opinion Today newsletter](#).*

A version of this article appears in print on April 10, 2018, on Page A27 of the New York edition with the headline: What Should They Ask Zuckerberg?. [Order Reprints](#) | [Today's Paper](#) | [Subscribe](#)

### It's Time to Break Up Facebook

The social media company has become a rogue actor, accountable to nobody.

By ERIC WILSON March 21, 2018

<https://www.politico.com/magazine/story/2018/03/21/its-time-to-break-up-facebook-217665>

Facebook is flailing amid the fallout from revelations about the alleged misuse of user data by Cambridge Analytica, the Trump campaign's 2016 data firm, dating back to 2014.

But the narrow focus on Cambridge Analytica and the Trump campaign misses the broader problem with Facebook and lacks fundamental context. Facebook is, to put the matter bluntly, a deeply untransparent, out-of-control company that encroaches on its users' privacy, resists regulatory oversight and fails to police known bad actors when they abuse its platform.

And it's not just Republicans who have taken advantage of Facebook's invasive features. Far from it: During the 2012 campaign, President Barack Obama's reelection team built an app that extracted the same types of data in the same fashion as the Cambridge Analytica data in question, with one critical difference: Obama's team extracted nearly five times the information.

According to Carol Davidsen, a member of Obama's data team, "Facebook was surprised we were able to suck out the whole social graph, but they didn't stop us once they realized that was what we were doing." The social graph is Facebook's map of relationships between users and brands on its platform. And after the election, she recently acknowledged, Facebook was "very candid that they allowed us to do things they wouldn't have allowed someone else to do because they were on our side."

There's been no word on whether the Obama team was asked to delete its data, nor has it been suspended from Facebook.

I've experienced Facebook's ineptitude and inconsistent policy enforcement firsthand, having served as digital director to Ed Gillespie's 2014 Senate campaign, Marco Rubio's 2016 presidential campaign and, most recently, Gillespie's 2017 campaign for governor. For example, in the 2017 Virginia Republican primary, on February 15, I flagged for Facebook's political team a post from a page supporting our opponent, Corey Stewart, that shared a link to a Washington Post article, but with an altered headline that gave users the impression that it was a legitimate headline from the Post.

The actual headline, referring to Stewart, read: "Protesters mob provocative Va. governor candidate [Stewart] as he defends Confederate statue," but the page used Facebook's headline editing feature (which has since been deactivated because of this incident) to say, "Gillespie: I'm OK with Charlottesville Taking Down the General Lee Monument."

It was the clearest case of false news I've seen and a perfect microcosm of the tactics that were employed by foreign actors during the 2016 presidential campaign.

For weeks, while this inaccurate headline was promoted to voters, misrepresenting Gillespie's position on a hot-button issue via Facebook ads, I was told by members of Facebook's U.S. Politics & Government Outreach team that nothing could be done. Finally, on March 21, 2017, when a reporter from The Associated Press contacted Facebook, the company decided that the post "violated Facebook's terms of not doing 'anything unlawful, misleading, malicious, or discriminatory.'" To my knowledge, Facebook never returned the money it received for the ads that violated its own policies.

The most frustrating aspect of dealing with Facebook is its infuriating inconsistency. The platform's terms of service are a sledgehammer when it needs it, but company executives apply them sparingly and without any clear consistency. Only when Facebook is confronted with the possibility of public scrutiny and bad coverage will it take action to do the right thing.

Facebook knew about the hundreds of apps that were extracting massive amounts of social graph data about its users dating back to its earliest days. Now, faced with a whistleblower, media exposés and a parliamentary inquiry, Facebook is only now taking action against a single entity for an incident that occurred years ago.

There's a constant thread, too, throughout all of Facebook's scandals, including the mishandling of the Russian interference in the 2016 election: It is an appallingly terrible corporate citizen.

Facebook makes millions of dollars every day selling its users' personal information, interests, political persuasions, location data, social relationships and internet history to advertisers who mix their content in with users' videos, photos, and posts. In return, users receive none of the revenue and yet bear many of the well-documented adverse effects, which include decreased well-being and self-esteem, lost friendships and a degraded civil society. Facebook has repeatedly shown itself incapable of behaving as a good corporate citizen and thus it is time the company is regulated and broken up.

I don't want to tar all of Silicon Valley with the same brush. New regulations can be narrowly targeted to Facebook, given its size and scope as a platform without hampering innovators across the industry who are behaving responsibly and ethically. Facebook has duopoly status (along with Google) in the advertising market, effective monopoly in the social media space and monopolies in many markets with its messaging platforms, like WhatsApp.

Regulation should include limits on the information Facebook may gather on its users and subsequently sell to advertisers, greater oversight and transparency related to its compliance with federal election laws and more cooperation with researchers about the adverse effects of its various platforms on individuals and communities. More broadly, the government should begin looking into breaking Facebook into smaller entities to allow for greater competition and more consumer-friendly practices in the online advertising, publishing and communications spaces.

For conservatives like me, it's not easy to call for increased regulation and antitrust enforcement, but Facebook has shown time and again that its leaders, including Mark Zuckerberg himself, aren't capable of responsibly wielding their immense power and influence in Americans' lives.

WASHINGTON  
LEGISLATIVE OFFICE.



April 9, 2018

**Re: Questions for Mark Zuckerberg**

Dear Representative,

On behalf of the American Civil Liberties Union (“ACLU”), we submit this letter for the record in connection with the House Committee on Energy and Commerce hearing, “Facebook: Transparency and Use of Consumer Data,” where Facebook Chairman and Chief Executive Officer Mark Zuckerberg is scheduled to testify.

Over the last month, the public has learned of various privacy breaches that have impacted tens of millions of Facebook users. The personal information of as many as 87 million people may have been improperly shared with Cambridge Analytica, which appears to have used this data to influence American voters.<sup>1</sup> Most Facebook users have reportedly had their public profile scraped for malicious purposes.<sup>2</sup> And, Facebook is currently being sued over concerns that it continues to fail to prevent ads that appear on the platform from improperly discriminating on the basis of gender, age, and other protected characteristics.<sup>3</sup> These incidents highlight both the existence of systemic deficiencies within Facebook and the need for stronger privacy laws in the U.S. to protect consumers.

We anticipate that members will question Mr. Zuckerberg regarding the recent incidents, the reasons Facebook has failed to adequately protect user privacy, and regulatory proposals the company will support. In addition to these topics, we urge you to ask Mr. Zuckerberg the following questions:

- Why has Facebook failed to take sufficient steps to ensure that advertisers do not wrongly exclude individuals from housing,

AMERICAN CIVIL  
LIBERTIES UNION  
WASHINGTON  
LEGISLATIVE OFFICE  
915 15th STREET, NW, 6<sup>TH</sup> FL  
WASHINGTON, DC 20005  
T/202.544.1681  
F/202.546.0738  
[WWW.ACLU.ORG](http://WWW.ACLU.ORG)

FAIZ SHAKIR  
DIRECTOR

NATIONAL OFFICE  
125 BROAD STREET, 18<sup>TH</sup> FL.  
NEW YORK, NY 10004-2400  
T/212.549.2500

OFFICERS AND DIRECTORS  
SUSAN N. HERMAN  
PRESIDENT

ANTHONY D. ROMERO  
EXECUTIVE DIRECTOR

ROBERT REMAR  
TREASURER

<sup>1</sup> Kurt Wagner, *Facebook says Cambridge Analytica may have had data from as many as 87 million people*, RECODE, April 4, 2018, <https://www.recode.net/2018/4/4/17199272/facebook-cambridge-analytica-87-million-users-data-collection> (last visited Apr 5, 2018).

<sup>2</sup> Tony Romm, Craig Timberg & Elizabeth Dwoskin, *Malicious Actors' used its tools to discover identities and collect data on a massive global scale*, WASHINGTON POST, April 5, 2018, [https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?utm\\_term=.31c3a8a679ee](https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?utm_term=.31c3a8a679ee) (last visited Apr 5, 2018).

<sup>3</sup> Charles Baglie, *Facebook Vowed to End Discriminatory Housing Ads. Suits Says it Didn't*, NEW YORK TIMES, March 27, 2018, available at <https://www.nytimes.com/2018/03/27/nyregion/facebook-housing-ads-discrimination-lawsuit.html> (last visited Apr 5, 2018).

employment, credit, and public accommodation ads based on gender, ethnic affinity, age, or other protected characteristics?

- Will Facebook provide privacy protections related to consent, retention, data portability, and transparency to American consumers that it will provide to EU consumers as a result of Europe’s law on data protection, the General Data Protection Regulation (“GDPR”)<sup>4</sup>, which will go into effect on May 25, 2018? In short, does Facebook plan to offer better privacy protection to Europeans than it does to Americans?

### 1. Facebook Ad Discrimination

Facebook offers advertisers many thousands of targeting categories, including those based on characteristics that are protected by civil rights laws — such as, gender, age, familial status, sexual orientation, disability, and veteran status — and those based on “proxies” for such characteristics. In the case of ads for housing, credit, and employment, discriminatory ad targeting and exclusion is illegal. Even outside these contexts, however, discriminatory targeting could raise civil rights concerns. For example, do we want any advertisers to be able to offer higher prices to individuals who Facebook believes are a particular race, or to exclude them from receiving ads offering certain commercial benefits?

Following complaints of discriminatory targeting, including efforts by the ACLU to raise concerns directly with the company, Facebook announced that it would no longer allow housing, credit, and employment ads targeted based on “affinity” for certain ethnic groups.<sup>5</sup> However, it did not prohibit targeting based on gender, age, veteran status, or other protected categories. These changes also did not address questions or concerns surrounding intentional targeting or exclusion of ads for public accommodations (for example, transportation). However, even after Facebook announced that it would no longer allow targeting of certain ads based on ethnic affinity, a ProPublica study found that the platform still failed to catch and prevent discriminatory ads that improperly excluded categories of users under the guise of targeting based on interests or affinity, including African Americans, Jewish people, and Spanish speakers.<sup>6</sup> Since then, Facebook has temporarily turned off ad targeting based on ethnic affinity until it can address these issues.<sup>7</sup>

<sup>4</sup>Regulation (EU) 2016/679 of the European Parliament and Council of the European Union on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter GDPR], April 27, 2016, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en>

<sup>5</sup> Erin Egan, *Improving Enforcement and Promoting Diversity: Updates to Ethnic Affinity Marketing*, FACEBOOK, Nov. 11, 2016, <https://newsroom.fb.com/news/2016/11/updates-to-ethnic-affinity-marketing/> (last visited Apr 6, 2018).

<sup>6</sup> Julia Angwin, Ariana Tobin & Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, ProPublica, PROPUBLICA, November 21, 2017, <https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin> (last visited Apr 5, 2018).

<sup>7</sup> Jessica Guynn, *Facebook halts ads that exclude racial and ethnic groups*, USA TODAY, Nov. 29, 2017, <https://www.usatoday.com/story/tech/2017/11/29/facebook-stop-allowing-advertisers-exclude-racial-and-ethnic-groups-targeting/905133001/> (last visited Apr 6, 2018).

Members should ask Zuckerberg why the platform has not turned off ad targeting for all protected categories or their proxies in the housing, credit, and employment, given that existing civil rights laws prohibit discriminatory ads in these contexts. In addition, they should question Zuckerberg regarding why the company has not taken sufficient steps – including increased auditing and facilitating research from independent entities – to assess and protect against discrimination outside of these contexts.

## 2. Privacy Protections Under the GDPR

For years, the ACLU has called on Facebook to provide more privacy protections to consumers and has emphasized the need for baseline privacy legislation in the U.S. With regards to Facebook, among other things, we have urged increased transparency, requirements that customers provide affirmative opt-in consent to share, use, or retain information, enhanced app privacy settings, auditing to assess third parties with access to Facebook, and other reforms. Many of these reforms have not been fully adopted, even in the wake of the Cambridge Analytica incident.<sup>8</sup>

However, some of these changes may soon be required for Facebook’s operation in the European Union as a result of Europe’s law on data protection, the GDPR, which will go into effect on May 25<sup>th</sup>. The GDPR does not provide an exact template for what baseline privacy regulation should look like in the U.S. – indeed, provisions such as the right to be forgotten would likely be unconstitutional if applied in the U.S. Nevertheless, there are elements of the GDPR that, if applied in the U.S., would help to ensure that Americans have full control over their data and are equipped with the tools necessary to safeguard their rights.

In recent statements, Zuckerberg has said that Facebook is working to extend a version of the GDPR that could be extended globally, but has failed to provide details regarding which provisions of the law will be applied to U.S. consumers.<sup>9</sup> Given this, members of Congress should press Zuckerberg on whether Facebook intends to voluntarily provide certain GDPR protections<sup>10</sup> to U.S. consumers, including:

- Consent Requirements: Absent certain exceptions,<sup>11</sup> the GDPR requires that companies obtain user consent to collect, use, or otherwise process their personal data.<sup>12</sup> This consent

<sup>8</sup> Nicole Ozer & Chris Conley, <https://www.aclu.org/blog/privacy-technology/internet-privacy/after-facebook-privacy-debacle-its-time-clear-steps-protect>, ACLU, Mar. 23, 2018, <https://www.aclu.org/blog/privacy-technology/internet-privacy/after-facebook-privacy-debacle-its-time-clear-steps-protect> (last visited Apr 6, 2018).

<sup>9</sup> David Ingreem & Joseph Menn, *Exclusive: Facebook CEO stops short of extending European privacy globally*, REUTERS, Apr. 3, 2018, <https://www.reuters.com/article/us-facebook-ceo-privacy-exclusive/exclusive-facebook-ceo-stops-short-of-extending-european-privacy-globally-idUSKCN1HA2M1> (last visited Apr 6, 2018).

<sup>10</sup> GDPR places different restrictions on entities based on whether they are “controllers” or “processors” of data. Facebook has stated that it acts as a controller for the majority of its business practices, though acts as a processor in certain instances when “working with business and third parties.” For purposes of this letter, we have included obligations on Facebook as both a controller and processor. See *What is the General Data Protection Regulation*, Facebook Business, available at <https://www.facebook.com/business/gdpr>.

<sup>11</sup> Other than consent, a company may process data to fulfill a contractual obligation to which the user is a party or to take steps at the request of the user prior to a contract; to comply with a legal obligation, to perform a task in the

must be freely given, specific, informed, and made by an affirmative action or statement by the user, and authorized by a parent/guardian if the user is under age 16.<sup>13</sup> If consent is written, the company must present the information in a manner that is intelligible, easily accessible, and uses clear and plain language. In addition, the user must have the right to withdraw their consent at any time.<sup>14</sup> In addition, processing of certain categories of sensitive data, like biometrics, religious beliefs, health data, and political opinions requires more rigorous “explicit consent.”

- **Data Portability:** GDPR provides users the right to obtain a copy of the data they have provided in a “structured, commonly used and machine-readable format” and to have this data transferred to another provider.<sup>15</sup>
- **Transparency:** GDPR states that companies collecting data must provide transparency regarding their data processes. Among other things, users are entitled to know the amount of time their personal data will be stored (or the criteria used to determine the retention period), categories of personal data collected, whether the provision of the data is a statutory or contractual requirement, the existence of automated decision making, who receives their personal data, and the purpose for which their personal data is being collected, used, or otherwise processed.<sup>16</sup> There are also similar transparency requirements in cases where an entity obtains personal data about an individual from a source other than the individual.<sup>17</sup>
- **Use of Data for Marketing:** GDPR provides user the right to object to use of their data for marketing purposes, including profiling for direct marketing purposes.<sup>18</sup>
- **Automated Decision-Making:** Absent certain exceptions (for example, explicit consent), GDPR states that users have the right to not be subject to decisions based solely on automated processing, including profiling, if it has a legal or similarly significant effect.<sup>19</sup>
- **Breach Notification:** In cases of any personal data breach, companies must notify a user if it is likely to result in a “high risk to the rights and freedoms” of individuals.<sup>20</sup> While the ACLU believes that notification should be required in circumstances far broader than this – and there are state laws that require notice in any case where there is a breach involving

---

public interest; to protect the vital interests of a data subject or other person; or to pursue a legitimate interest unless the interests are overridden by the interests/rights of the data subject. See GDRP, *supra* note 4, art. 6.

<sup>12</sup> *Id.*

<sup>13</sup> *Id.* at art. 4. GDPR permits members states to provide a lower age, no younger than 13, for consent purposes. See *Id.* at art. 6.

<sup>14</sup> *Id.* at art. 7.

<sup>15</sup> *Id.* at art. 20.

<sup>16</sup> *Id.* at art. 12.

<sup>17</sup> *Id.* at art. 14.

<sup>18</sup> *Id.* at art. 21.

<sup>19</sup> *Id.* at art. 22.

<sup>20</sup> *Id.* at art. 34.

certain types of personal data<sup>21</sup> – the GDPR breach policy could be a step forward in cases where there is not more protective applicable U.S. law.

Voluntary application of GDPR requirements by companies to U.S. consumers cannot be a substitute for baseline privacy legislation in the U.S., which must include enforcement mechanisms, redress in the case of breaches, and a private right of action not subject to mandatory arbitration. Until such legislation, however, voluntary application of these rights could help to safeguard users in the U.S.

If you have questions, please contact ACLU Legislative Counsel, Neema Singh Guliani, at 202-675-2322 or [nguliani@aclu.org](mailto:nguliani@aclu.org).

Sincerely,



Faiz Shakir  
National Political Director



Neema Singh Guliani  
Legislative Counsel

---

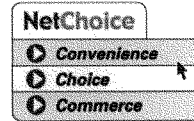
<sup>21</sup> See California Civ. Code s. 1798.82(a).



**NetChoice** *Promoting Convenience, Choice, and Commerce on The Net*

Carl Szabo, Vice President and General Counsel  
1401 K St NW, Suite 502  
Washington, DC 20005  
202-420-7485  
[www.netchoice.org](http://www.netchoice.org)

April 9, 2018  
SUBMITTED ELECTRONICALLY



**NetChoice Comments for the Record for  
US House of Representatives Energy & Commerce Committee Hearing:  
*Facebook: Transparency and Use of Consumer Data***

NetChoice respectfully submits the following comments for the record regarding the US House of Representatives Energy & Commerce Committee hearing: *Facebook: Transparency and Use of Consumer Data*.

NetChoice is a trade association of leading e-commerce and online companies. We work to promote the integrity and availability of the global internet and are significantly engaged in privacy issues in the states, in Washington, and in international internet governance organizations.

Through these comments we seek to clarify the potential harm to America's businesses from aggressive laws and regulations on online platforms. For example, taking a European approach<sup>1</sup> on interest-based ads would cost American businesses \$340 billion over the next five years. Consumers would also have a worse user experience accompanied with less relevant advertising.

Likewise, limitations on large online platforms will impact the small and mid-size businesses who rely on the size and scope of these platforms to reach customers and grow their business.

**Eliminating interest-based ads by default will cost American businesses and make it harder for Americans to access content**

Calls to limit or eliminate interest-based ads by default, like the BROWSER Act,<sup>2</sup> would erase up to \$340 billion in advertising revenue from American websites over the next five years.<sup>3</sup> This means potentially less content, more ads, and/or more paywalls.

Requiring users to opt-in to interest-based advertising and studies have shown that such an opt-in regime reduces online ads' effectiveness by 65 percent. This precipitous drop in ad effectiveness means a likewise drop in revenue for American businesses and a worse user experience.

<sup>1</sup> See, European Privacy and Electronic Communications Directive 2002/58/EC.

<sup>2</sup> Balancing the Rights of Web Surfers Equally and Responsibly Act of 2017, H. R. 2520 (May 18, 2018).

<sup>3</sup> See Analysis at <https://netchoice.org/library/loss-of-340-billion/>.

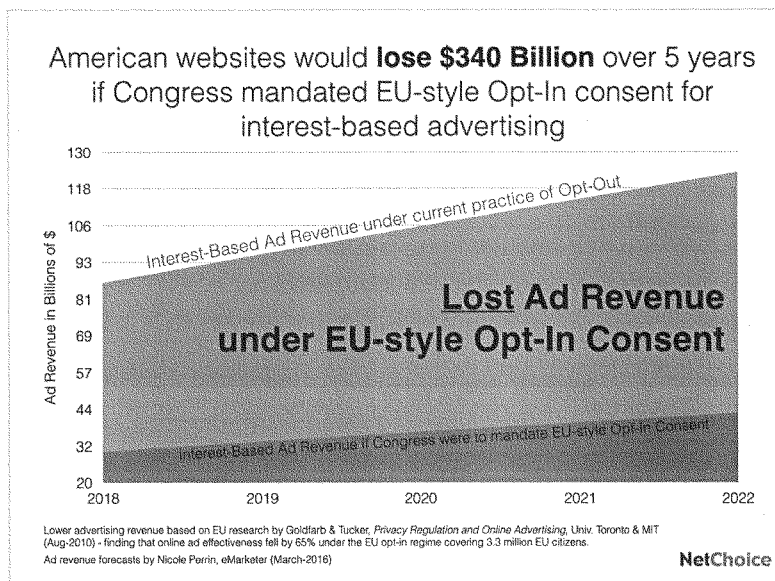
There is an old adage:

“Half the money spent on advertisements is wasted, I just don’t know which half.”

This quote represents a problem from a by-gone era where only mass-media advertisements were really possible – think TV commercials, radio spots, and newspaper ads. With these ads, the likelihood that the viewer is interested in the ad is likely low resulting in inefficient advertising expenses.

Conversely, interest-based ads enable small businesses to better spend their limited advertising dollars. Studies have shown that interest-based advertisements are 65% more effective than contextual ads.<sup>4</sup> Interest-based ads help small businesses show potential customers products they actually want and allows small businesses to use more money to grow their business and hire new employees.

Taking actions to return to the old-school advertising model will fall hard on for small businesses.



It’s not just American businesses that lose with such restrictions, but also American consumers visiting websites. Because of \$340 billion price tag for such advertising restrictions, we’ll see one or more of these consequences:

- Websites will show more ads to make up lost revenue.
- Websites will have less to spend on reporters, content, services, and innovation.
- Some websites will erect paywalls for content that users get for free today.

<sup>4</sup> Goldfarb & Tucker, *Privacy Regulation and Online Advertising*, Univ. Toronto & MIT (Aug-2010) - finding that online ad effectiveness fell by 65% under the EU opt-in regime covering 3.3 million EU citizens.

These consequences are bad for American consumers, and especially harmful for low-income households that can't afford to pay for online services.

### **America's small businesses and organizations rely on online platforms**

Erasing \$340 billion of revenue from American websites hits small businesses and small organizations the hardest, since they depend on low-cost and effective interest-based advertising to reach new customers and engage with existing ones. This connection is especially important for small and mid-size businesses who may have neither the name recognition nor the funds to afford traditional advertising.

Think back twenty years ago, when new businesses spread the word through expensive broadcast and newspaper advertising and direct mail campaigns. This was costly and not particularly effective, since advertisers were unable to effectively target viewers and households who had an interest in their products.

But online platforms have revolutionized advertising for small businesses and non-profit organizations. Using online platforms, small businesses now connect with potential customers at a fraction of the cost they would have historically paid.

National advertising used to be restricted to all but the wealthiest companies. Using online platforms, now any business of any size can advertise across the country. Of course, the larger the platform, the easier it is for America's small businesses to connect with those most likely to be interested.

A recent survey by Morning Consult<sup>5</sup> found that:

- 84% of small enterprises use at least one major digital platform to provide information to customers
- 70% of small businesses said that Facebook helps them attract new customers

There are many examples of small businesses leveraging online platforms in every part of America.

#### ***All Things Real Estate in Portland, OR***

For a couple of dollars, this small business can reach their target audience with ads. The female-owned business used Facebook to increase sales by 500% in less than 10 months by connecting with likely customers.

Owner Tracey Hicks said, "Many of our customers tell us they saw our ads on Facebook or saw another realtor wearing our products and ask us for the same. If it wasn't for our Facebook ads we wouldn't be as big as we are now."

#### ***CandyLipz LLC. in San Francisco, CA***

Facing declining revenue, owner Thienna Ho turned to online platforms to help her businesses. As a result, she has grown her business from three to fifteen employees in 15 months.

#### ***Lost Cabin Beer Co. in Rapid City, SD***

Realizing that legacy media was cost-prohibitive and ineffective, this small beverage company leveraged online platforms to find customers and grow their business.

<sup>5</sup> Examining the Impact of Technology on Small Businesses, available at [https://www.uschamber.com/sites/default/files/ctec\\_sme-rpt\\_v3.pdf](https://www.uschamber.com/sites/default/files/ctec_sme-rpt_v3.pdf)

**Sons & Daughters Farm and Winery in West Palm Beach, FL**

Following Hurricane Katrina, this family farm was decimated. Using online platforms, this small family business was able to reinvigorate their wine business and is now also hosting parties and weddings at their farm.

**Bluntzer Fruit Stand in Robstown, TX**

This business of farmers leveraged online platforms to reach customers who would never have otherwise visited their farm.

One founder said that because of online platforms, “I am never out of reach of my customers or their needs. The fruit stand may close at 6 p.m., but our customer service department is open 24/7. I think our clients really enjoy that about us.”

Platforms also help smaller enterprises to find new employees and help job-seekers to find work. Large online platforms like LinkedIn and ZipRecruiter rely on their large platforms to quickly connect employers with ideal candidates.

With over 8 million job listings and over 7 million active job seekers each month, ZipRecruiter connects 80% of employers with quality candidates within 24 hours.<sup>6</sup> Of course, the larger the platform, the easier it is for businesses and potential employees to connect.

**Online platforms are already subject to hundreds of laws and regulations**

Today, every online platform is subject to multiple laws and regulations, including 47 state laws regarding data breaches and over a hundred state and federal privacy laws and regulations.

Take for example Section 5 of the Federal Trade Commission (“FTC”) Act, which prohibits “unfair or deceptive trade practices.”<sup>7</sup> This broad enforcement power enables the FTC to take action against online platforms that fail to honor their terms-of-service or privacy promises.<sup>8</sup> Likewise, the FTC has used its unfairness enforcement power to take action against businesses that fail to adequately protect data.<sup>9</sup>

Moreover, Section 5 of the FTC Act is enforceable by the Federal Trade Commission and by every state Attorney General under the “little Section 5” authority.

Other laws which regulate online platforms include, the Children’s Online Privacy Protection Act,<sup>10</sup> California’s Online Privacy Protection Act,<sup>11</sup> California’s Privacy Rights for California Minors in the Digital

<sup>6</sup> See, e.g., About Us – Ziprecruiter, <https://www.ziprecruiter.com/about>.

<sup>7</sup> Federal Trade Commission Act, 15 USC §45 (“FTC Act”), “The Commission is hereby empowered and directed to prevent [use of] unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.”

<sup>8</sup> See, e.g. *In the Matter of Nomi Technologies, Inc.*, Matter No. 1323251 (Apr. 2015). The FTC found that a technical error in Nomi’s privacy policy was enough for an enforcement action even though the FTC couldn’t show a single consumer misunderstood or suffered any harm.

<sup>9</sup> See *In the Matter of ASUSTeK Computer, Inc.*, Complaint, FTC Dkt. No. C-4587 (July 18, 2016) (company’s cloud storage service, offered in connection with sale of internet routers, was allegedly insecure).

<sup>10</sup> 15 U.S.C. 6501–6505

<sup>11</sup> Calif. Bus. & Prof. Code §§ 22575–22578

World Act,<sup>12</sup> Delaware’s Online and Personal Privacy Protection,<sup>13</sup> and the Pennsylvania Deceptive or fraudulent business practices law,<sup>14</sup> to name a few.

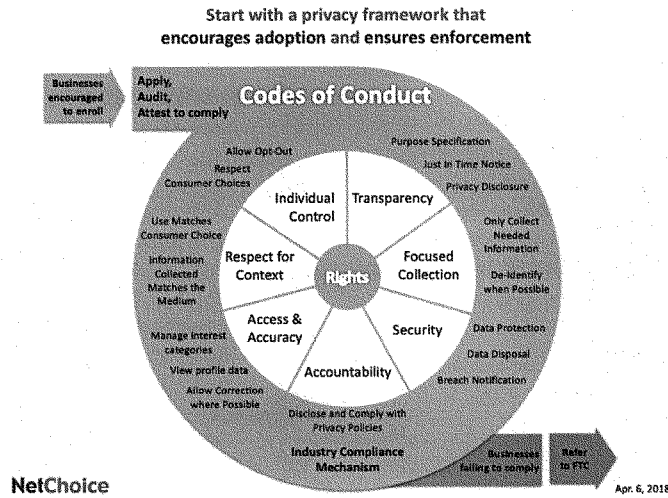
Clearly, the suggestion that “internet platforms are unregulated” is inaccurate.

**Role for Government**

The role for government should be where consumers cannot adequately act to protect their privacy interests, through choices they alone can make. Government should use its powers to pursue online fraud and criminal misuse of data, not to create rules that narrowly prescribe how data should be used.

Overall, we support the notion that businesses and customers – not governments – must take the lead on data privacy. Businesses need to pursue innovation without repeatedly asking for permission from government agencies. And consumers must understand the decisions they make and must be allowed to make those decisions.

We offer this conceptual view of an industry self-regulatory framework that dynamically adapts to new technologies and services, encourages participation, and enhances compliance.



As seen in the conceptual overview, components of the Privacy Bill of Rights form the aspirational core that influences business conduct regarding data privacy. From previous work by the FTC, NAI, and IAB, we’ve established the foundational principles for the collection and use of personal information:

<sup>12</sup> Calif. Bus. & Prof. Code §§ 22580-22582

<sup>13</sup> Del. Code § 19-7-705

<sup>14</sup> 18 Pa. C.S.A. § 4107(a)(10)

individual control, transparency, respect for context, access and accuracy, focused collection, accountability, and security.

Participating companies would publicly attest to implement Codes within their business operations, including periodic compliance reviews. If a company failed to comply with the adopted Codes, the FTC and state Attorneys General could bring enforcement actions, as is currently the case when companies fail to honor their adopted privacy policies.

We thank the Committee for giving us the opportunity to present our concerns and look forward to further discussions about this important topic.

Sincerely,

Carl Szabo  
Vice President and General Counsel, NetChoice  
*NetChoice is a trade association of e-Commerce and online businesses. [www.netchoice.org](http://www.netchoice.org)*



**Vietnam Veterans of America**

8719 Colesville Road, Suite 100, Silver Spring, MD 20910 • Telephone (301) 585-4000  
Fax (301) 585-0519 • Advocacy (301) 585-3180 • Communications (301) 585-2691  
www.vva.org

April 5, 2018

Chairman Greg Walden  
c/o: Nolan Ahern, Military/Veterans  
Legislative Assistant  
Personal Office Staff  
U.S. House Committee on Energy and  
Commerce  
2125 Rayburn House Office Building  
Washington, D.C. 20515

Ranking Member Frank Pallone, Jr.  
c/o: James Johnson, Military/Veterans  
Legislative Assistant  
Personal Office Staff  
U.S. House Committee on Energy and  
Commerce  
2125 Rayburn House Office Building  
Washington, D.C. 20515

**Re: Foreign Entities Imitating American Veterans Organizations and Sowing Discord with Falsified or Manipulated News**

Dear Chairman Walden and Ranking Member Pallone,

We are writing to bring the attention of the Committee to an issue of national security. Here we are presenting evidence of a foreign entity (or entities) operating on Facebook, Twitter and Instagram with the intent to infiltrate and influence the community of American Veterans online. Similar to widely-reported stories of “troll farms” sowing discord during the 2016 election cycle and specifically targeting veterans,<sup>1</sup> these online entities operate by first appealing to patriotic Americans, and once they have gained the trust of tens or hundreds of thousands of followers, they begin spreading manipulated and divisive news and other political content.

Vietnam Veterans of America (VVA) is a congressionally chartered Veteran Service Organization whose membership exceeds 80,000 Vietnam Veterans living around the globe. For many of our aging and disabled veterans, their most significant connection to VVA and the outside world is through use of the internet and social media platforms. According to a recent Oxford study, veterans are trusted by the civilian populace as opinion leaders, which makes us a

---

<sup>1</sup> Schreckinger, Ben, et al. “How Russia Targets the U.S. Military.” *POLITICO Magazine*, POLITICO LLC, 12 June 2017, [www.politico.com/magazine/story/2017/06/12/how-russia-targets-the-us-military-215247](http://www.politico.com/magazine/story/2017/06/12/how-russia-targets-the-us-military-215247).

natural target for influence.<sup>2</sup> It is for the protection of our veterans, and the sanctity of the American electorate that we urge you to investigate this issue and take appropriate proactive measures to ensure a safe and trustworthy cyber environment for American veterans.

On August 21, 2017, we discovered a Facebook page titled “*Vietnam Vets of America*,”<sup>3</sup> which had at times been using our logo and registered trademark to deceive its online audience into thinking it was an affiliate of our legitimate veterans service organization.<sup>4</sup> Posts from “*Vietnam Vets of America*” typically linked to “*vvets.eu*,” a website anonymously registered<sup>5</sup> through Netfinity JSC<sup>6</sup> of Bulgaria. After filing complaints for copyright infringements via Facebook’s Help tools, we monitored the page for activity, and reached out directly to report the suspicious page to a member of Facebook’s Security Team on August 23, 2017.<sup>7</sup>

While most of the posts shared on “*Vietnam Vets of America*” were junk memes of no significance, the page did occasionally share deceptive or manipulated news and political content that was likely shared to incite an emotional reaction from veterans. On September 26, 2017, the page shared a manipulated video using “Facebook Live,” which streamed a looped 58-second long clip about a Vietnam Veterans monument being defaced for approximately four hours.<sup>8</sup> We immediately reported this to Facebook’s Security Team, and logged a complaint for “spam” via Facebook’s video reporting function. The original video had been produced by News 22 WWLP, a local news station from Springfield Massachusetts,<sup>9</sup> however, a caption was inserted by “*Vietnam Vets of America*” over the video that said “DO YOU THINK THE CRIMINALS MUST SUFFER?” with icons encouraging people to respond with the “heart” and “angry-face” reactions. Over the course of the four-hour video — thousands of shares, comments and reactions were produced — taking advantage of Facebook’s algorithms which promote popular

<sup>2</sup> John D. Gallacher, Vlad Barash, Philip N. Howard, and John Kelly. “Junk News on Military Affairs and National Security: Social Media Disinformation Campaigns Against US Military Personnel and Veterans.” *Data Memo* 2017.9. Oxford, UK: *Project on Computational Propaganda*. Comprop.oi.ox.ac.uk. <http://comprop.oi.ox.ac.uk/research/working-papers/vetops/>

<sup>3</sup> Web address: <https://www.facebook.com/americanvvets/>. This page has since been taken down by Facebook, but is likely recoverable by Facebook, Inc for the purposes of research and investigation. See *Addendum 1* for screenshot of “*Vietnam Vets of America*” Facebook homepage.

<sup>4</sup> Evidence of the use of our logo was deleted by the “*Vietnam Vets of America*” Facebook Page after our communications staff filed a complaint to the anonymous page administrator. Below is evidence of the same entity using our trademark on a different Facebook page.

<sup>5</sup> DomainTools. “Whois Record for VVets.eu.” *Domain Tools WhoIs Records*, 20 Mar. 2018, [www.whois.domaintools.com/vvets.eu](http://www.whois.domaintools.com/vvets.eu).

<sup>6</sup> “NETFINITI” EAD. “Netfinity Home Page.” *Netfinity.bg*, 20 Mar. 2018, [www.netfinity.bg/](http://www.netfinity.bg/).

<sup>7</sup> Email traffic with a representative of Facebook’s security team will be presented to investigators upon request.

<sup>8</sup> This video has since been taken down by Facebook, but is likely recoverable by Facebook, Inc for the purposes of research and investigations. See *Addendum 2* for screenshot. Web address: <https://www.facebook.com/americanvvets/videos/1722930374682550/>

<sup>9</sup> See *Addendum 3* for screenshot. Caron, Matt. “Black Vietnam Veterans Monument in Springfield Vandalized.” *WWLP.com*, Nexstar Broadcasting, Inc., 26 Sept. 2017, [www.wwlp.com/2017/09/25/black-vietnam-veterans-monument-in-springfield-vandalized/](http://www.wwlp.com/2017/09/25/black-vietnam-veterans-monument-in-springfield-vandalized/).



“live” videos, increasing the likelihood that people who didn’t yet “like” or follow the page would be exposed to it. This video contained a link to the *vvets.eu* website, which copied the written content of News 22 WWLP’s reporting.<sup>10</sup> By October 3, 2017, the manipulated video had been viewed over 37,000 times.

Other divisive, political content that was shared by “*Vietnam Vets of America*” included the NFL “Take a Knee” and boycott controversies<sup>11</sup> and “Blue Lives Matter.”<sup>12</sup> While these types of memes were popular among Americans on social media, their use by a foreign entity is consistent with information warfare tactics described in the Russian book *Information-Psychological War Operations: A Short Encyclopedia and Reference Guide*.<sup>13</sup>

The rate at which the “*Vietnam Vets of America*” page grew in followers is staggering. According to their “About” page, they went from 30,000 followers on November 1, 2016, to 196,567 as of October 2017.<sup>14</sup>

On October 9, 2017, after having not found a solution through talks with Facebook’s Security Team, VVA began to go public via the press with appeals to the Department of Defense (DoD) and the Department of Veterans Affairs (VA) to take proactive measures to protect servicemembers and veterans online from foreign political influence.<sup>15</sup> On October 18, 2017, Facebook responded to questioning by *Stars and Stripes* regarding our specific complaints by saying that the “*Vietnam Vets of America*” page had not violated Facebook terms of use,<sup>16</sup> and placed the burden on VVA to speak out and educate Facebook users of the imposter page.

<sup>10</sup> Anonymous “Administrator,” *vvets.eu/author/nmitow*. “Vietnam Veterans Monument in Springfield Vandalized.” *Vietnam Vets of America*, 26 Sept. 2017, *vvets.eu/vietnam-veterans-monument-springfield-vandalized/*.

<sup>11</sup> “NFL Boycott” post has since been removed, although Facebook may have the ability to restore it. <https://www.facebook.com/americanvvets/posts/1723531927955728>

<sup>12</sup> “Blue Lives Matter” post has since been removed, although Facebook may have the ability to restore it. <https://www.facebook.com/americanvvets/posts/1721512648157656>

<sup>13</sup> From *The Guardian*: “The book is designed for “students, political technologists, state security services and civil servants” – a kind of user’s manual for junior information warriors. The deployment of information weapons, it suggests, “acts like an invisible radiation” upon its targets: “The population doesn’t even feel it is being acted upon. So the state doesn’t switch on its self-defence mechanisms.” If regular war is about actual guns and missiles, the encyclopedia continues, “information war is supple, you can never predict the angle or instruments of an attack.” Source: <https://www.theguardian.com/news/2015/apr/09/kremlin-hall-of-mirrors-military-information-psychology>

<sup>14</sup> This page has since been removed by Facebook. Several other milestones of audience growth were posted there. [https://www.facebook.com/pg/americanvvets/about/?ref=page\\_internal](https://www.facebook.com/pg/americanvvets/about/?ref=page_internal)

<sup>15</sup> Shane, Leo. “Report: Online Trolls Targeting US Troops, Veterans.” *Military Times*, Military Times, 10 Oct. 2017, [www.militarytimes.com/veterans/2017/10/10/report-online-trolls-targeting-us-troops-veterans/](http://www.militarytimes.com/veterans/2017/10/10/report-online-trolls-targeting-us-troops-veterans/).

<sup>16</sup> Wentling, Nikki. “Veterans Organization Asks for More Help Combating ‘Imposter’ Facebook Page.” *Stars and Stripes*, Stars and Stripes, 18 Oct. 2017, [www.stripes.com/news/veterans-organization-asks-for-more-help-combating-imposter-facebook-page-1.493168](http://www.stripes.com/news/veterans-organization-asks-for-more-help-combating-imposter-facebook-page-1.493168).

On October 24, 2017, Facebook removed the suspect page for violation of copyright, though no information was publicly shared regarding who had been operating the page.<sup>17</sup> At a November 1, 2017 hearing before the Senate Intelligence Committee on Russian interference in America's election on social media, Facebook's lawyer, Colin Stretch, denied knowledge of the imposter VVA page or efforts to target veterans when questioned directly on the matter by Senator Joe Manchin of West Virginia.<sup>18</sup> Mr Stretch did not promise specific efforts by Facebook to counteract such deception aimed at veterans.

As of the writing of this report, DoD and VA have yet to respond to VVA's request that they coordinate federal efforts to protect servicemembers and veterans from deceptive, foreign-generated online content.

On February 21, 2018, we became aware of two new Facebook pages, "*Nam Vets*" and "*Vietnam-Veterans.org*," which link to "*vvets.eu*" as well as a sister site, *Vietnam-Veterans.org*, which uses a similar logo<sup>19</sup> and posts identical content.<sup>20</sup> According to the About section of the "*Nam Vets*" Facebook page, they had reached 500 followers on November 24, 2017, and they now have 3,044 followers.<sup>21</sup> The Facebook page "*Vietnam-Veterans.org*" first posted on December 10, 2017,<sup>22</sup> and they now have 155 followers. Although these pages have relatively few followers, they have an engaged audience, who often respond to posts asking for them to divulge information, such as what unit they served with and when they were deployed.

We have opted not to file complaints with Facebook at this time, as their simply shutting down pages does not prevent others from rising in their place, nor does it allow us to find out who is behind them or what their motivations are.

Like the now defunct "*Vietnam Vets of America*" page, the "*Nam Vets*" Facebook page began by using VVA's logo to gain trust from American veterans.<sup>23</sup> According to the timestamp on the

<sup>17</sup> Wentling, Nikki. "Facebook Shuts down 'Imposter' Veterans Page." *Stars and Stripes*, Stars and Stripes, 25 Oct. 2017, [www.stripes.com/facebook-shuts-down-imposter-veterans-page-1.494404](http://www.stripes.com/facebook-shuts-down-imposter-veterans-page-1.494404).

<sup>18</sup> "Hearing: Social Media Influence in the 2016 U.S. Elections." *Hearings | Intelligence Committee*, U.S. Senate Select Committee on Intelligence, 1 Nov. 2017, [www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections](http://www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections).

<sup>19</sup> See Addendum 3 for comparison of "*vvets.eu*" and "*Vietnam-Veterans.org*" logos.

<sup>20</sup> "Home Page." *Veterans of America*, 20 Mar. 2018, [vietnam-veterans.org/](http://vietnam-veterans.org/).

<sup>21</sup> "*Nam Vets*" Facebook page is <https://www.facebook.com/Nam-Vets-241974999306216/> and

"*Vietnam-Veterans.org*" Facebook page is <https://www.facebook.com/vietnamveterans.org/>.

<sup>22</sup> "Facebook Post." *Vietnam-Veterans.org Updated Their Cover Photo*, *Vietnam-Veterans.org* Facebook Page, 10 Dec. 2017, [www.facebook.com/vietnamveterans.org/posts/1741676985864149](http://www.facebook.com/vietnamveterans.org/posts/1741676985864149).

<sup>23</sup> See Addendum 4 for screenshot of "*Nam Vets*" using VVA's trademarked logo. "Facebook Post," *Nam Vets Updated Their Cover Photo*, *Nam Vets* Facebook Page, 17 Apr. 2015. <https://www.facebook.com/241974999306216/photos/a.241975099306206.1073741825.241974999306216/241975105972872/?type=1&theater>.

post with our logo, the “*Nam Vets*” Facebook page existed as early as April 17, 2015. Its first posts links to a now archived website containing inflammatory political content such as videos of protesters stomping on American flags.<sup>24</sup> Content more recently posted on the Facebook pages and affiliated websites includes pictures and videos of Veterans Memorials being defaced (with deceptive dating to make these events appear more recent),<sup>25</sup> a video produced by the Department of Veterans Affairs,<sup>26</sup> and the illegally copied text<sup>27</sup> of an article written by Nikki Wentling of *Stars and Stripes*<sup>28</sup> regarding cuts to veterans benefits (which was posted well after it was current news).<sup>29</sup>

The new site “*Vietnam-Veterans.org*” is registered to one Nikola Mitov, also through Netfinity JSC of Bulgaria.<sup>30</sup> When searching the street address (“210 6-th september BLVD”) for the registrant provided on the Internet Corporation for Assigned Names and Numbers (ICANN) website, the street address shows up in Ukraine,<sup>31</sup> rather than Bulgaria as listed — although this may be due to translation errors or limitations of Google Maps. Both Bulgaria<sup>32</sup> and Ukraine<sup>33</sup> have struggled to control online trolls who work to promote pro-Russian disinformation.

<sup>24</sup> “Archived page: [EXCLUSIVE]Veteran arrested for defending the American flag from stomping[EXCLUSIVE],” *Wayback Machine*, Internet Archive, 20 Mar. 2018, <https://web.archive.org/web/20150630003749/http://skivai.eu:80/537>.

<sup>25</sup> Video comprised of still images of a defaced Vietnam Veterans Memorial. *Nam Vets*. “*Nam Vets Facebook Video*.” *Nam Vets - SHOCKING! ΔThe Memorial Wall in Venice, LA Is...*, Facebook, 2017, [www.facebook.com/241974999306216/videos/474542656049448/](http://www.facebook.com/241974999306216/videos/474542656049448/).

<sup>26</sup> The video on the “*Nam Vets*” Facebook page was originally produced by Department of Veterans Affairs Explore.VA.gov website. Copied content: “*Nam Vets*.” *Nam Vets - ΔEvery Veteran Must Read This!Δ Read More...*, Facebook, 2017, [www.facebook.com/241974999306216/videos/10156145737652558/](http://www.facebook.com/241974999306216/videos/10156145737652558/). Original web location of content: Department of Veterans Affairs. “*Explore VA Benefits Overview*.” *The Official YouTube Channel for the U.S. Department of Veterans Affairs*, YouTube, 19 June 2015, [www.youtube.com/watch?v=pOLGDmtn8sU&feature=youtu.be](http://www.youtube.com/watch?v=pOLGDmtn8sU&feature=youtu.be) <https://explore.va.gov/video-gallery>.

<sup>27</sup> Copied text. Anonymous “Administrator,” *vvets.eu/author/macman*. “*Cuts to VA Programs*.” *Vietnam Veterans of America*, 6 July 2017, [vvets.eu/cuts-va-programs/](http://vvets.eu/cuts-va-programs/).

<sup>28</sup> Original content from *Stars and Stripes* as posted on *Military.com*. Wentling, Nikki. “*Budget Calls for Cuts to VA Programs as Tradeoff for Extending Choice*.” *Military.com*, *Stars and Stripes*, 23 May 2017, [www.military.com/daily-news/2017/05/23/budget-calls-cuts-va-programs-tradeoff-extending-choice.html](http://www.military.com/daily-news/2017/05/23/budget-calls-cuts-va-programs-tradeoff-extending-choice.html).

<sup>29</sup> See Addendum 5 for December 27, 2017 posting of the copied *Stripes* article that was originally written on May 23, 2017.

<sup>30</sup> Internet Corporation for Assigned Names and Numbers. “*ICANN WHOIS Records for VIETNAM-VETERANS.ORG*.” *ICANN WHOIS*, Internet Corporation for Assigned Names and Numbers, 20 Mar. 2018, [www.whois.icann.org/en/lookup?name=vietnam-veterans.org](http://www.whois.icann.org/en/lookup?name=vietnam-veterans.org).

<sup>31</sup> Google. “*Google Maps*.” *Google Maps*, 20 Mar. 2018, [www.google.com/maps/qABVB7PAY2O2](http://www.google.com/maps/qABVB7PAY2O2). Search query: “210 6-th september BLVD, Plovdiv Plovdiv 4000 BG”.

<sup>32</sup> Colborne, Michael. “*Made in Bulgaria: Pro-Russian Propaganda*.” *Coda Story*, Coda Media, Inc., 9 May 2017, [www.codastory.com/disinformation-crisis/foreign-proxies/made-in-bulgaria-pro-russian-propaganda](http://www.codastory.com/disinformation-crisis/foreign-proxies/made-in-bulgaria-pro-russian-propaganda).

<sup>33</sup> Collins, Ben, and Katie Zavadski. “*Zuckerberg Blew Off Russian Troll Warnings Before the Attack on America*.” *The Daily Beast*, The Daily Beast Company, 27 Sept. 2017, [www.thedailybeast.com/zuckerberg-blew-off-warnings-of-russian-trolls-in-2015](http://www.thedailybeast.com/zuckerberg-blew-off-warnings-of-russian-trolls-in-2015).

The “*Vietnam-Veterans.org*” entity is now spread across at least two new social media platforms, including Twitter<sup>34</sup> and Instagram.<sup>35</sup> We do not know if the “*Nam Vets*” or “*Vietnam Vets of America*” Facebook pages have or had affiliated accounts across other social media platforms, but suspect that this entity has been operating consistently.

On behalf of the 80,000+ members of Vietnam Veterans of America, we are requesting the assistance of your committee in investigating the use of social media by foreign actors to target and influence American Veterans. As social media becomes evermore important to the daily lives of all generations of veterans, we hope to see the government take a proactive approach to ensuring a safe cyber environment. Should you have questions on this matter, please feel free to contact Kristofer Goldsmith, Assistant Director for Policy and Government Affairs at [kgoldsmith@vva.org](mailto:kgoldsmith@vva.org) or 516-457-1260.

Sincerely,



John Rowan  
National President and CEO  
Vietnam Veterans of America

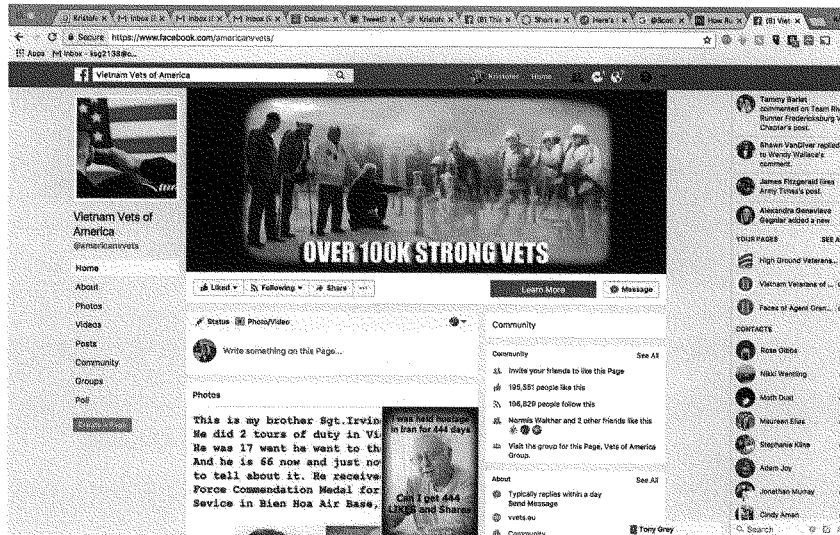
Cc:  
U.S. Senate Committee on Homeland Security and Governmental Affairs  
U.S. House Committee on Oversight and Government Reform  
U.S. Senate Committee on Intelligence  
U.S. House Permanent Select Committee on Intelligence  
U.S. Senate Committee on Veterans' Affairs  
U.S. House Committee on Veterans' Affairs  
U.S. Senate Committee on Armed Services  
U.S. House Committee on Armed Services  
U.S. Senate Committee on the Judiciary  
U.S. House Committee on the Judiciary

<sup>34</sup> Vietnam-veterans.org. “Vietnam-Veterans.org (@Vietnamvetsorg).” *Twitter*, Twitter, 13 Mar. 2018, [www.twitter.com/vietnamvetsorg](http://www.twitter.com/vietnamvetsorg).

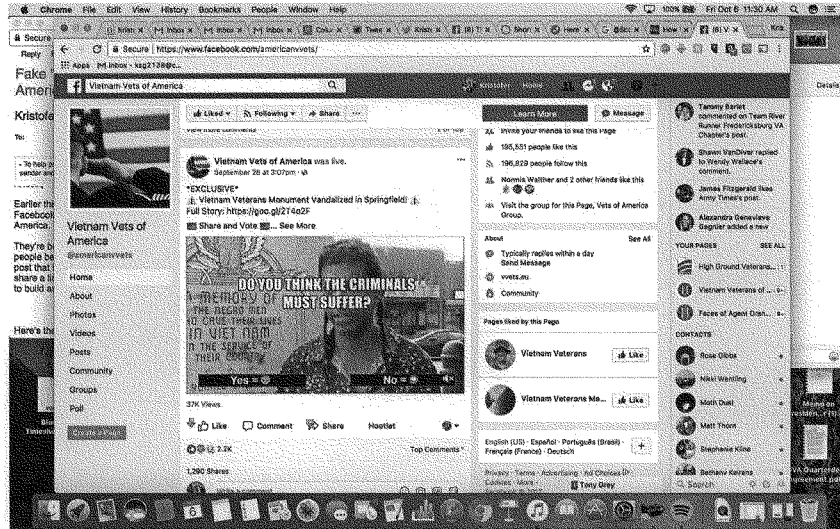
<sup>35</sup> “Veterans of America (@Vietnamveteransorg) • Instagram Photos and Videos.” *Instagram*, Instagram, 20 Mar. 2018, [www.instagram.com/vietnamveteransorg/](http://www.instagram.com/vietnamveteransorg/).

U.S. Department of Defense  
U.S. Federal Bureau of Investigation  
U.S. Federal Trade Commission  
U.S. Department of Homeland Security

**Addendum 1:** Screenshot of “Vietnam Vets of America” Facebook Page.



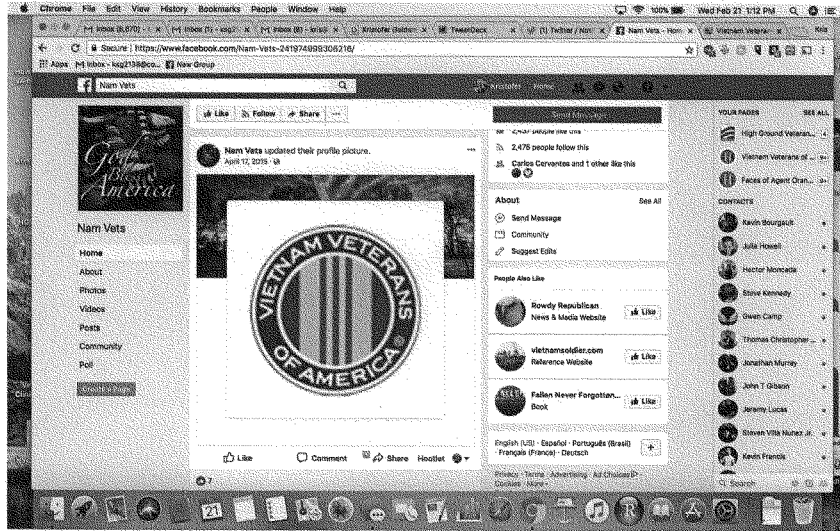
**Addendum 2:** Screenshot of “Vietnam Vets of America” September 26, 2017 “Facebook Live” video which was pre-recorded and had the caption “Do you think the criminals must suffer?”



**Addendum 3:** New logo for “Vietnam-Veterans.org” compared to logo of “Vietnam Vets of America.”



**Addendum 4:** Screenshot of “Nam Vets” Facebook page using VVA’s registered trademark and logo.





**Addendum 5:** Sharing of news content regarding proposed cuts to veterans benefits six months after the fact is a deceptive use of facts which is likely to incite reactions from the veteran community. December 27, 2017 posting of the copied *Stars and Stripes* article that was originally written on May 23, 2017.





April 11, 2018

The Honorable Greg Walden  
 Chairman  
 House Energy & Commerce Committee  
 2185 Rayburn House Office Building  
 Washington, DC 20515

The Honorable Frank Pallone  
 Ranking Member  
 House Energy & Commerce Committee  
 237 Cannon House Office Building  
 Washington, DC 20515

Dear Chairman Walden and Ranking Member Pallone,

On behalf of Public Knowledge, a public interest advocacy organization dedicated to promoting freedom of expression, an open internet, and access to affordable communications tools and creative works, we applaud the House Energy & Commerce Committee for holding a hearing on "Facebook: Transparency and Use of Consumer Data." We appreciate the opportunity to submit this letter for the record.

The Facebook disclosures over the last several weeks have been unrelenting. First, we learned that an app developer, Aleksandr Kogan, funneled personal information about at least 87 million Facebook users to Cambridge Analytica, a firm that purported to engage in "psychographics" to influence voters on behalf of the Trump campaign. Gallingly, as was Facebook's practice for all apps at that time, when users connected Kogan's app to their Facebook accounts, the app scooped up not only the users' personal information, but also their friends' information – without any notice to the friends or opportunity for the friends to consent. We then learned that Facebook had been collecting Android users' SMS and call histories. While Android users may have technically consented to that data collection, the outrage this news provoked strongly suggests that the notice Facebook provided about the practice was insufficient to permit users to understand precisely to what they were consenting. Last week, we learned that "malicious actors" used Facebook's search tools to build profiles of individuals whose e-mail addresses and phone numbers had been stolen in data breaches over the years and posted on the dark web. These profiles enabled identity theft.

But Facebook is hardly unique. In the twenty-first century, it is impossible to meaningfully participate in society without sharing our personal information with third parties. We increasingly live our lives online. We turn to platforms and companies to access education, health care, employment, the news, and emergency communications. We shop online. When we seek to rent a new apartment, buy a home, open a credit card, or, sometimes, apply for a job, someone checks our credit scores through companies on the internet. These third party companies and platforms should have commensurate obligations to protect our personal information, and those obligations must have the force of law. Unfortunately, it has become increasingly clear that too many third parties fail to live up to this responsibility. Rather, unauthorized access to personal data has run rampant – whether it is in the form of Cambridge Analytica, where authorized access to data was misused and shared in ways that exceeded authorization, or in the form of a data breach, where information was accessed in an unauthorized way. Just since the Cambridge Analytica news broke, consumers have learned of data breaches at Orbitz, Under Armour, Lord and Taylor, Saks Fifth Avenue, Saks Off Fifth, Panera Bread, Sears Holding Corp., and Delta Airlines.

We have also learned about purportedly authorized access to data that many consumers find unsavory and would likely not consent to, if they were clearly and fully informed of the nature of the transaction. For example, last week, we learned that Grindr has been sharing its users' HIV status with two other companies, Apptimize and Localytics. This sharing is almost certainly disclosed in Grindr's terms of service, but it is well known that few people read terms of service, and there is good reason to believe that had Grindr been upfront about this data sharing practices, few of its users would have agreed to it.

The industry has long insisted that it can regulate itself. However, the deluge of data breaches and unauthorized and unsavory use of consumer data makes clear that self-regulation is insufficient. Indeed, Facebook was already under a consent decree with the Federal Trade Commission (FTC), and yet it still failed to protect its users' personal information.

This hearing is a good start to begin addressing corporate collection and use of user data in the modern economy. But, a hearing alone is not enough. We hope that the Committee will use this hearing to build the record for strong, comprehensive privacy legislation. Here are three elements that any privacy legislation should include:

#### **Notice and Consent**

Until the digital age, individual ownership and control of one's own personal information was the basis for privacy law in the United States.<sup>1</sup> We should return to this principle. While we cannot avoid sharing information with some third parties, we can have greater control over that information. At a minimum, consumers should have a right to know a) what information is being collected and retained about them; b) how long that information is being retained; c) for what purposes that information is being retained; d) whether the retained information is identifiable, pseudo-anonymized, or anonymized; e) whether and how that information is being used; f) with whom that information is being shared; g) for what purposes that information is being shared; h) under what rubric that information is being shared (for free, in exchange for compensation, subject to a probable cause warrant, etc.); and (i) whether such information is being protected with industry recognized best practices.

It is imperative that this notice be meaningful and effective, which means that it cannot be buried in the fine print of a lengthy privacy policy or terms of service agreement. Consumers and companies know that consumers do not typically read privacy policies or terms of service agreements. Indeed, researchers at Carnegie Mellon estimate that it would take seventy-six work days for an individual to read all of the privacy policies she encounters in a year.<sup>2</sup> Companies take advantage of this common knowledge to bury provisions that they know consumers are unlikely to agree to in the fine print of these agreements. While courts have found these agreements to be binding contract, there is no reason that Congress cannot undo this presumption and insist that notice be provided in a way that consumers can quickly read and understand.

<sup>1</sup> HAROLD FELD, *PRINCIPLES FOR PRIVACY LEGISLATION: PUTTING PEOPLE BACK IN CONTROL OF THEIR INFORMATION* 19 – 20 (Public Knowledge, 2017).

<sup>2</sup> Alexis C. Madrigal, *Reading the Privacy Policies you Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC, Mar. 1, 2012, <https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/>.

Moreover, notice alone is insufficient. Consumers must also have meaningful opportunities to freely and affirmatively consent to data collection, retention, and sharing. And, that consent should be as granular as possible. For example, a user should be able to consent for her data to be used for research purposes, but not for targeted advertising – or vice-versa. As with notice, the consent must be real rather than implied in the fine print of a terms of service. Consumers must also have the ability to withdraw their consent if they no longer wish for a company to use and retain their personal data, and they should be able to port their data in a machine-readable format to another service, if they so desire. In addition, service should not be contingent on the sharing of data that is not necessary to render the service.<sup>3</sup>

The General Data Protection Regulation, which goes into effect in Europe in May, will require some kinds of granular notice and consent, so companies already have to figure out how to offer their users opportunities for meaningful consent. There is no reason for them not to offer the same opportunities for meaningful notice and consent in the United States.

### **Security Standards**

Organizations that are stewards of our personal information should be expected to adhere to recognized best practices to secure the information. This is particularly true when an individual cannot avoid sharing the information without foregoing critical services or declining to participate in modern society.

Relatedly, organizations should be required to adhere to privacy by design and by default and to practice data minimization. The presumption should be that only data necessary for the requested transaction will be retained, absent explicit consumer consent. Organizations should be encouraged to employ encryption, pseudo-anonymization, and anonymization to protect consumers' private information, and security mechanisms should be regularly evaluated. Importantly, these evaluations must be publicly conducted, with the government acting as convener of any multi-stakeholder process. Facebook/Cambridge Analytica, as well as the cascade of recent data breaches, has demonstrated that industry cannot be trusted to police itself.

### **Meaningful Recourse**

When there is unauthorized access to personal information, individuals must be made whole to the greatest extent possible. There are two major barriers to this. The first is the Federal Arbitration Act, which requires courts to honor the forced arbitration clauses in contracts, including forced arbitration clauses buried in the fine print of terms of service agreements. Forced arbitration clauses require consumers to settle any dispute they have with a company by arbitration rather than having their day in court – and often consumers do not even know an arbitration clause

<sup>3</sup> While it may be appropriate for a non-essential service like Facebook to charge users a fee in lieu of selling their data, see Alex Johnson and Erik Ortiz, *Without data-targeted ads, Facebook would look like a pay service, Sandberg says*, NBC NEWS, Apr. 5, 2018, <https://www.nbcnews.com/tech/social-media/users-would-have-pay-opt-out-all-facebook-ads-sheryl-n863151>, such an approach is unacceptable for services that are integral for participation in society. Individuals should be able to access health care, education, housing, and other essential services without compromising their personal information or having to pay extra for their fundamental right to privacy.

is in their contract until they go to sue. This presents three problems: 1) Arbitrators are often more sympathetic to large companies, who are repeat players in the arbitration system, than most juries would be. 2) Arbitration creates no legal precedent. 3) Frequently, it is not cost-effective for an individual to bring a claim against a large company by herself. The damages she could win likely would not exceed her legal costs. But, when customers can band together in a class action lawsuit, it becomes much more feasible to bring a case against a large company engaged in bad behavior. Forced arbitration clauses preclude class action. Congress should explicitly exempt cases addressing the failure to protect personal information from the Federal Arbitration Act to make sure consumers can have their day in court when their information is misused and their trust abused.

The other major barrier to meaningful recourse is the difficulty calculating the damages associated with unauthorized access to personal information. While one may be able to quantify her damages when her credit card information is breached or her identity is stolen, it is much harder to do so in a situation like Facebook/Cambridge Analytica. It is difficult to put a dollar amount on having one's privacy preferences ignored or her personal information revealed to third parties without her knowledge or consent. We instinctively know that there is harm in having one's personal data used for "psychographics" to influence her behavior in the voting booth, but that harm is difficult to quantify. Congress already uses liquidated damages in other situations when the damage is real, but hard to quantify. In fact, liquidated damages are already used to address other privacy harms. For example, the Cable Privacy Act provides for liquidated damages when cable companies impermissibly share or retain personally identifiable information.

While the FTC can step in when companies engage in unfair and deceptive practices, the FTC is likely to only intervene in the most egregious cases. Moreover, the FTC can only extract damages from companies once they have violated users' privacy once, entered into a consent decree with the Agency, and then violated the consent decree. That means a lot of consumers have to have their personal information abused before a company is held to account. Moreover, when the FTC is involved, any damages go to the government, not to making individuals whole.

We are not recommending that the FTC be taken out of the business of protecting consumers in the digital age, but merely suggesting that consumers should also have the opportunity to protect themselves. Allowing private, class action lawsuits for liquidated damages when companies fail to safeguard private information will create the necessary incentives for companies to take appropriate precautions to protect the information they have been entrusted with. Companies, after all, understand the technology and the risks, and are in the best position to develop safeguards to protect consumers.

#### **Existing Laws and Legislation**

While we hope that Congress will use this hearing to build the record for comprehensive privacy legislation, we encourage Congress to enact legislation that is compatible with existing federal sector-specific privacy laws in communications, health care, finance, and other sectors, as well as with state and local privacy laws. While the federal government should set minimum standards of protection for all Americans, states have been in the vanguard of privacy protection and are much-needed "cops on the beat." Even if Congress were to dramatically expand the resources

available to federal privacy agencies, the federal government could not hope to provide adequate protection to consumers on its own. Rather, the states, as laboratories of democracy, should be empowered to innovate and provide greater privacy protections to their residents.

These sector-specific privacy laws and state privacy laws, as well as legislation, introduced in this Congress and in previous Congresses, addressing notice and consent, security requirements, data breaches, and/or forced arbitration may be good building blocks for comprehensive legislation. But, Congress must ensure that the bills are updated to address today's harms. For example, many of the bills that have been drafted narrowly define personal information to include identifiers like first and last name, social security numbers, bank account numbers, etc. These bills would not personally cover the personal information in question in Facebook/Cambridge Analytica – information like social media “likes” that is certainly useful for influencing an individual in the voting booth, as well as for more mundane marketing and advertising purposes, and that, when aggregated, may, in fact, be personally identifiable.

#### **Conclusion**

Again, we appreciate the opportunity to submit this letter for the record for the House Energy & Commerce Committee hearing on “Facebook: Transparency and Use of Consumer Data” We look forward to continuing the conversation and stand ready to assist interested Members in crafting consumer privacy protection legislation. If you have any questions or would like more information, please do not hesitate to reach out to me at [aboehm@publicknowledge.org](mailto:aboehm@publicknowledge.org).

Sincerely,



Allison S. Bohm  
Policy Counsel  
Public Knowledge

CC. Members of the House Energy & Commerce Committee

**epic.org**

Electronic Privacy Information Center  
1718 Connecticut Avenue NW, Suite 200  
Washington, DC 20009, USA

+1 202 483 1140  
+1 202 483 1248  
@EPICPrivacy  
<https://epic.org>

April 10, 2018

The Honorable Greg Walden, Chair  
The Honorable Frank Pallone, Ranking Member  
U.S. House Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, D.C. 20515

Dear Members of the House Energy & Commerce Committee:

We write to you regarding tomorrow's hearing on "Facebook: Transparency and Use of Consumer Data."<sup>1</sup> We appreciate your interest in this important issue. For many years, the Electronic Privacy Information Center ("EPIC") has worked with the House Energy & Commerce Committee to help protect the privacy rights of Americans.<sup>2</sup>

In this statement from EPIC, we outline the history of Facebook's 2011 Consent Order with the Federal Trade Commission, point to key developments (including the failure of the FTC to enforce the Order), and make a few preliminary recommendations. Our assessment is that the Cambridge Analytica breach, as well as a range of threats to consumer privacy and democratic institutions, could have been prevented if the Commission had enforced the Order.

EPIC would welcome the opportunity to testify, to provide more information, and to answer questions you may have. Our statement follows below.

**EPIC, the 2011 FTC Consent Order, and Earlier Action by the FTC**

Facebook's transfer of personal data to Cambridge Analytica was prohibited by a Consent Order the FTC reached with Facebook in 2011 in response to an extensive investigation

<sup>1</sup> *Facebook: Transparency and Use of Consumer Data*, 115th Cong. (2018), H. Comm. on Energy & Commerce, <https://energycommerce.house.gov/hearings/facebook-transparency-use-consumer-data/> (April 11, 2018).

<sup>2</sup> See, e.g. Marc Rotenberg, EPIC Executive Director, Testimony before the House Comm. on Energy & Commerce, Subcomm. on Communications and Technology, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows* (November 13, 2015), <https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf>; Marc Rotenberg, EPIC Executive Director, Testimony before the House Comm. on Energy & Commerce, Subcomm. on Communications and Technology, *Communications Networks and Consumer Privacy: Recent Developments* (April 23, 2009), [https://epic.org/privacy/dpi/rotenberg\\_HouseCom\\_4-09.pdf](https://epic.org/privacy/dpi/rotenberg_HouseCom_4-09.pdf); Letter from EPIC to the House Comm. on Energy and Commerce on FCC Privacy Rules (June 13, 2016), <https://epic.org/privacy/consumer/EPIC-FCC-Privacy-Rules.pdf>.

EPIC Statement  
House Energy & Commerce Committee

1

Facebook and Privacy  
April 10, 2018

**Privacy is a Fundamental Right.**

and complaint pursued by EPIC and several US consumer privacy organizations.<sup>3</sup> The FTC's failure to enforce the order we helped obtain has resulted in the unlawful transfer of 87 million user records to a controversial data mining firm to influence a presidential election as well as the vote in Brexit. The obvious question now is "why did the FTC fail to act?" The problems were well known, widely documented, and had produced a favorable legal judgement in 2011.

Back in 2007, Facebook launched Facebook Beacon, which allowed a Facebook user's purchases to be publicized on their friends' News Feed after transacting with third-party sites.<sup>4</sup> Users were unaware that such features were being tracked, and the privacy settings originally did not allow users to opt out. As a result of widespread criticism, Facebook Beacon was eventually shutdown.

In testimony before the Senate Commerce Committee in 2008, we warned about Facebook's data practices:

Users of social networking sites are also exposed to the information collection practices of third party social networking applications. On Facebook, installing applications grants this third-party application provider access to nearly all of a user's information. Significantly, third party applications do not only access the information about a given user that has added the application. Applications by default get access to much of the information about that user's friends and network members that the user can see. This level of access is often not necessary. Researchers at the University of Virginia found that 90% of applications are given more access privileges than they need.<sup>5</sup>

Nonetheless in February 2009, Facebook changed its Terms of Service. The new TOS allowed Facebook to use anything a user uploaded to the site for any purpose, at any time, even after the user ceased to use Facebook. Further, the TOS did not provide for a way that users could completely close their account. Rather, users could "deactivate" their account, but all the information would be retained by Facebook, rather than deleted.

EPIC planned to file an FTC complaint, alleging that the new Terms of Service violated the FTC Act Section 5, and constituted "unfair and deceptive trade practices." In response to this planned complaint, and a very important campaign organized by the "Facebook Users Against the New Terms of Service," Facebook returned to its previous Terms of Service. Facebook then

<sup>3</sup> Fed. Trade Comm'n., *In re Facebook*, Decision and Order, FTC File No. 092 3184 (Jul. 27, 2012) (Hereinafter "Facebook Consent Order"), <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf>.

<sup>4</sup> EPIC, Social Networking Privacy, <https://epic.org/privacy/socialnet/>.

<sup>5</sup> *Impact and Policy Implications of Spyware on Consumers and Businesses: Hearing Before the S. Comm. on Commerce, Science, and Transportation 110th Cong. (2008)* (statement of Marc Rotenberg, Exec. Dir. EPIC) (C-SPAN video at <https://www.c-span.org/video/?205933-1/computer-spyware>), [https://www.epic.org/privacy/dv/Spyware\\_Test061108.pdf](https://www.epic.org/privacy/dv/Spyware_Test061108.pdf).



established a comprehensive program of Governing Principles and a statement of Rights and Responsibilities.<sup>6</sup>

As we reported in 2009:

Facebook has announced the results of the vote on site governance. The initial outcome indicates that approximately 75 percent of users voted for the new terms of service which includes the new Facebook Principles and Statement of Rights and Responsibilities. Under the new Principles, Facebook users will "own and control their information." Facebook also took steps to improve account deletion, to limit sublicenses, and to reduce data exchanges with application developers. EPIC supports the adoption of the new terms. For more information, see EPIC's page on Social Networking Privacy.<sup>7</sup>

However, Facebook failed to uphold its commitments to a public governance structure for the company.

From mid-2009 through 2011, EPIC and a coalition of consumer organizations pursued comprehensive accountability for the social media platform.<sup>8</sup> When Facebook broke its final commitment, we went ahead with a complaint to the Federal Trade Commission. Our complaint alleged that Facebook had changed user privacy settings and disclosed the personal data of users to third parties without the consent of users.<sup>9</sup> EPIC and others had conducted extensive research and documented the instances of Facebook overriding the users' privacy settings to reveal personal information and to disclose, for commercial benefit, user data, and the personal data of friends and family members, to third parties without their knowledge or affirmative consent.<sup>10</sup>

<sup>6</sup> *Facebook takes a Democratic Turn*, USA Today, Feb. 27, 2009, at 1B, <https://www.pressreader.com/usa/usa-today-us-edition/20090227/281887294213804>

<sup>7</sup> EPIC, *Facebook Gets Ready to Adopt Terms of Service* (Apr. 24, 2009) <https://epic.org/2009/04/facebook-gets-ready-to-adopt-t.html>

<sup>8</sup> There is a longer history of significant events concerning the efforts of Facebook users to establish democratic accountability for Facebook during the 2008-2009 period. The filing of the 2009 complaint came about after it became clear that Facebook would not uphold its commitments to the Statement of Right and Responsibilities it had established. It would also be worth reconstructing the history of the "Facebook Users Against the New Terms of Service" as Facebook destroyed the group and all records of its members and activities after the organizers helped lead a successful campaign against the company. Julius Harper was among the organizers of the campaign. A brief history was written by Ben Popken in 2009 for *The Consumerist*, "What Facebook's Users Want In The Next Terms Of Service," <https://consumerist.com/2009/02/23/what-facebooks-users-want-in-the-next-terms-of-service/>. Julius said this in 2012: "Most people on Facebook don't even know they can vote or even that a vote is going on. What is a democracy if you don't know where the polling place is? Or that a vote is even being held? How can you participate? Ignorance becomes a tool that can be used to disenfranchise people." *Facebook upsets some by seeking to take away users' voting rights*, San Jose Mercury News, Nov. 30, 2012, <https://www.mercurynews.com/2012/11/30/facebook-upsets-some-by-seeking-to-take-away-users-voting-rights/>.

<sup>9</sup> *In re Facebook*, EPIC.org, <https://epic.org/privacy/inrefacebook/>.

<sup>10</sup> *FTC Facebook Settlement*, EPIC.org, <https://epic.org/privacy/ftc/facebook/>.

We explained our argument clearly in the 2009 EPIC complaint with the Commission (attached in full to this statement):

This complaint concerns material changes to privacy settings made by Facebook, the largest social network service in the United States, which adversely impact users of the Facebook service. Facebook's changes to users' privacy settings disclose personal information to the public that was previously restricted. Facebook's changes to users' privacy settings also disclose personal information to third parties that was previously not available. These changes violate user expectations, diminish user privacy, and contradict Facebook's own representations. These business practices are Unfair and Deceptive Trade Practices, subject to review by the Federal Trade Commission (the "Commission") under section 5 of the Federal Trade Commission Act.<sup>11</sup>

We should also make clear that the 2009 complaint that EPIC filed with the Federal Trade Commission about Facebook was not the first to produce a significant outcome. In July and August 2001, EPIC and a coalition of fourteen leading consumer groups filed complaints with the Federal Trade Commission (FTC) alleging that the Microsoft Passport system violated Section 5 of the Federal Trade Commission Act (FTCA), which prohibits unfair or deceptive practices in trade.<sup>12</sup>

EPIC and the groups alleged that Microsoft violated the law by linking the Windows XP operating system to repeated exhortations to sign up for Passport; by representing that Passport protects privacy, when it and related services facilitate profiling, tracking and monitoring; by signing up Hotmail users for Passport without consent or even the ability to opt-out; by representing that the system complies with the Children's Online Privacy Protection Act; by not allowing individuals to delete their account; and by representing that the system securely holds individuals' data.

We requested that the FTC initiate an investigation into the information collection practices of Windows XP and other services, and to order Microsoft to revise XP registration procedures; to block the sharing of Passport information among Microsoft properties absent explicit consent; to allow users of Windows XP to gain access to Microsoft web sites without disclosing their actual identity; and to enable users of Windows XP to easily integrate services provided by non-Microsoft companies for online payment, electronic commerce, and other Internet-based commercial activity.

The Federal Trade Commission undertook the investigation we requested and issued an important consent order. As the Commission explained announcing its enforcement action in 2002:

<sup>11</sup> *In the Matter of Facebook, Inc.* (EPIC, Complaint, Request for Investigation, Injunction, and Other Relief) before the Federal Trade Commission, Washington, D.C. (filed Dec. 17, 2009), <http://www.epic.org/privacy/infacebook/EPIC-FacebookComplaint.pdf>.

<sup>12</sup> EPIC, *Microsoft Passport Investigation Docket*, <https://epic.org/privacy/consumer/microsoft/passport.html>.

Microsoft Corporation has agreed to settle Federal Trade Commission charges regarding the privacy and security of personal information collected from consumers through its "Passport" web services. As part of the settlement, Microsoft will implement a comprehensive information security program for Passport and similar services. . . .

The Commission initiated its investigation of the Passport services following a July 2001 complaint from a coalition of consumer groups led by the Electronic Privacy Information Center (EPIC).

According to the Commission's complaint, Microsoft falsely represented that:

- It employs reasonable and appropriate measures under the circumstances to maintain and protect the privacy and confidentiality of consumers' personal information collected through its Passport and Passport Wallet services, including credit card numbers and billing information stored in Passport Wallet;
- Purchases made with Passport Wallet are generally safer or more secure than purchases made at the same site without Passport Wallet when, in fact, most consumers received identical security at those sites regardless of whether they used Passport Wallet to complete their transactions;
- Passport did not collect any personally identifiable information other than that described in its privacy policy when, in fact, Passport collected and held, for a limited time, a personally identifiable sign-in history for each user; and
- The Kids Passport program provided parents control over what information participating Web sites could collect from their children.

The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years.<sup>13</sup>

FTC Chairmen Timothy J. Muris said at the time, "Good security is fundamental to protecting consumer privacy. Companies that promise to keep personal information secure must follow reasonable and appropriate measures to do so. It's not only good business, it's the law. Even absent known security breaches, we will not wait to act."<sup>14</sup>

<sup>13</sup> Fed. Trade Comm'n, *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises: Passport Single Sign-In, Passport "Wallet," and Kids Passport Named in Complaint Allegations*, Press Release, (Aug. 8, 2002), <https://www.ftc.gov/news-events/press-releases/2002/08/microsoft-settles-ftc-charges-alleging-false-security-privacy>.

<sup>14</sup> *Id.*

Then in December 2004, EPIC filed a complaint with the Federal Trade Commission against databroker Choicepoint, urging the Commission to investigate the compilation and sale of personal dossiers by data brokers such as Choicepoint.<sup>15</sup> Based on the EPIC complaint, in 2005, the FTC charged that Choicepoint did not have reasonable procedures to screen and verify prospective businesses for lawful purposes and as a result compromised the personal financial records of more than 163,000 customers in its database. In January 2006, the FTC announced a settlement with Choicepoint, requiring the company to pay \$10 million in civil penalties and provide \$5 millions for consumer redress. EPIC's Choicepoint complaint produced the largest civil fine at the time in the history of the FTC.<sup>16</sup>

The Microsoft order led to user-centric identity scheme that, if broadly adopted, could have done much to preserve the original open, decentralized structure of the Internet. The Choicepoint order led to significant reforms in the data broker industry. And it is worth noting that both investigations were successfully pursued with Republican chairmen in charge of the federal agency and both actions were based on unanimous decisions by all of the Commissioners.

The Facebook complaint should have produced an outcome even more consequential than the complaints concerning Microsoft and Choicepoint. In 2011, the FTC, based the materials we provided in 2009 and 2010, confirmed our findings and recommendations. In some areas, the FTC even went further. The FTC issued a Preliminary Order against Facebook in 2011 and then a Final Order in 2012.<sup>17</sup> In the press release accompanying the settlement, the FTC stated that Facebook "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public."<sup>18</sup>

According to the FTC, under the proposed settlement Facebook is:

- "barred from making misrepresentations about the privacy or security of consumers' personal information;"
- "required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences;"
- "required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;"

<sup>15</sup> EPIC, ChoicePoint, <https://www.epic.org/privacy/choicepoint/>

<sup>16</sup> Fed. Trade Comm'n., *ChoicePoint Settles Data Security Breach Charges: to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress: At Least 800 Cases of Identity Theft Arose From Company's Data Breach* (Jan. 26, 2006), <https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million>.

<sup>17</sup> Facebook Consent Order.

<sup>18</sup> Fed. Trade Comm'n., *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises*, Press Release, (Nov. 29, 2011), <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>.

- “required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers’ information; and”
- “required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers’ information is protected.”<sup>19</sup>

The reporting requirements are set out in more detail in the text of the Final Order. According to the Final Order:

[The] Respondent [Facebook] shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain controls and procedures appropriate to Respondent’s size and complexity, the nature and scope of Respondent’s activities, and the sensitivity of the covered information, including:

- A. the designation of an employee or employees to coordinate and be responsible for the privacy program.
- B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent’s unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.
- C. the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures.
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.

<sup>19</sup> *Id.*

- E. the evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.<sup>20</sup>

Moreover, the Final Order stated:

Respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons selected to conduct such Assessments and prepare such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. Any decision not to approve a person selected to conduct such Assessments shall be accompanied by a writing setting forth in detail the reasons for denying such approval. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific privacy controls that Respondent has implemented and maintained during the reporting period;
- B. explain how such privacy controls are appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information;
- C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of this order; and
- D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the order is terminated

<sup>20</sup> Facebook Consent Order.

and provided to the Associate Director of Enforcement within ten (10) days of request.<sup>21</sup>

EPIC expressed support for the Consent Order but also believed it could be improved.<sup>22</sup> In response to the FTC's request for public comments on the proposed order we wrote:

EPIC supports the findings in the FTC Complaint and supports, in part, the directives contained in the Consent Order. The Order makes clear that companies should not engage in unfair and deceptive trade practices, particularly in the collection and use of personal data. However, the proposed Order is insufficient to address the concerns originally identified by EPIC and the consumer coalition, as well as those findings established by the Commission. Consistent with this earlier determination, to protect the interests of Facebook users, and in light of recent changes in the company's business practices, EPIC urges the Commission to require Facebook to:

- Restore the privacy settings that users had in 2009, before the unfair and deceptive practices addressed by the Complaint began;
- Allow users to access all of the data that Facebook keeps about them;
- Cease creating facial recognition profiles without users' affirmative consent;
- Make Facebook's privacy audits publicly available to the greatest extent possible;
- Cease secret post-log out tracking of users across web sites.

At the time, the FTC settlement with Facebook was widely viewed as a major step forward for the protection of consumer privacy in the United States. The Chairman of the FTC stated, "Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users. Facebook's innovation does not have to come at the expense of consumer privacy. The FTC action will ensure it will not." Mark Zuckerberg said at the time of the Consent Order that the company had made "a bunch of mistakes."<sup>23</sup> The FTC Chair called Mr.

<sup>21</sup> *Id.* at 6-7.

<sup>22</sup> Comments of EPIC, *In the Matter of Facebook, Inc.*, FTC File No. 092 3184, (Dec. 27, 2011), <https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf>.

<sup>23</sup> Somini Sengupta, *F.T.C. Settles Privacy Issue at Facebook*, N.Y. Times, at B1 (Nov. 29, 2011), <https://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html>. There was also a "lengthy blog post" from Mr. Zuckerberg in the N.Y. Times article but the link no longer goes to Mr. Zuckerberg's original post. Mr. Zuckerberg's post in 2009 that established the Bill of Rights and Responsibilities for the site has also disappeared. This is the original link: <http://blog.facebook.com/blog.php?post=54746167130>.

Zuckerberg's post a "good sign" and said, "He admits mistakes. That can only be good for consumers."<sup>24</sup>

Commissioners and staff of the FTC later testified before Congress, citing the Facebook Consent Order as a major accomplishment for the Commission.<sup>25</sup> And U.S. policymakers held out the FTC's work in discussions with trading partners for the proposition that the US could provide privacy protections to those users of US-based services. For example, former FTC Chairwoman wrote this to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission:

As part of its privacy and security enforcement program, the FTC has also sought to protect EU consumers by bringing enforcement actions that involved Safe Harbor violations. . . . Twenty-year consent orders require Google, Facebook, and Myspace to implement comprehensive privacy programs that must be reasonably designed to address privacy risks related to the development and management of new and existing products and services and to protect the privacy and confidentiality of personal information. The comprehensive privacy programs mandated under these orders must identify foreseeable material risks and have controls to address those risks. The companies must also submit to ongoing, independent assessments of their privacy programs, which must be provided to the FTC. The orders also prohibit these companies from misrepresenting their privacy practices and their participation in any privacy or security program. This prohibition would also apply to companies' acts and practices under the new

<sup>24</sup> Julianne Pepitone, *Facebook settles FTC charges over 2009 privacy breaches*, CNN Money (Nov. 29, 2011), [http://money.cnn.com/2011/11/29/technology/facebook\\_settlement/index.htm](http://money.cnn.com/2011/11/29/technology/facebook_settlement/index.htm).

<sup>25</sup> According to the statement of the FTC Commissioners who testified before the Senate Commerce Committee in 2012:

Similar to the Google order, the Commission's consent order against Facebook prohibits the company from deceiving consumers with regard to privacy; requires it to obtain users' affirmative express consent before sharing their information in a way that exceeds their privacy settings; and requires it to implement a comprehensive privacy program and obtain outside audits. In addition, Facebook must ensure that it will stop providing access to a user's information after she deletes that information.

*The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission: Hearing Before the S. Comm on Commerce, Science and Transportation*, at 18, 112th Cong. (May 9, 2012) (statement of Fed. Trade Comm'n.), [https://www.ftc.gov/sites/default/files/documents/public\\_statements/prepared-statement-federal-trade-commission-need-privacy-protections-perspectives-administration-and/120509privacyprotections.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-need-privacy-protections-perspectives-administration-and/120509privacyprotections.pdf), see also, *The Need for Privacy Protections*:

*Perspectives from the Administration and the Federal Trade Commission, Hearing before the S. Comm. on Commerce, Science, and Transportation, 112th Cong. (May 19, 2012)* (statement of Maureen K. Ohlhausen, Commissioner, Fed. Trade Comm'n) ("We have also charged companies with failing to live up to their privacy promises, as in the highly publicized privacy cases against companies such as Google and Facebook, which together will protect the privacy of more than one billion users worldwide. As a Commissioner, I will urge continuation of this strong enforcement record."), [https://www.ftc.gov/sites/default/files/documents/public\\_statements/statement-commissioner-maureen-k.ohlhausen/120509privacystatement.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-k.ohlhausen/120509privacystatement.pdf).



Privacy Shield Framework. . . . Consequently, these FTC orders help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe.<sup>26</sup>

Yet the Federal Trade Commission never charged Facebook with a single violation of the 2011 Consent Order.

**The Google Consent Order and the FTC's Subsequent Failure to Enforce Consent Orders**

In 2011, we also had also obtained a significant consent order at the FTC against Google after the disastrous roll-out of Google "Buzz." In that case, the FTC established a consent order after Google tried to enroll Gmail users into a social networking service without meaningful consent. The outcome was disastrous. Personal contact information was made publicly available by Google as part of its effort to establish a social network service to compete with Facebook. EPIC filed a detailed complaint with the Commission in February that produced a consent order in 2011, comparable to the order for Facebook.<sup>27</sup>

But a problem we did not anticipate became apparent almost immediately: the Federal Trade Commission was unwilling to enforce its own consent orders. Almost immediately after the settlements, both Facebook and Google began to test the FTC's willingness to stand behind its judgements. Dramatic changes in the two companies' advertising models led to more invasive tracking of Internet users. Online and offline activities were increasingly becoming merged.

To EPIC and many others, these changes violated the terms of the consent orders. We urged the FTC to establish a process to review these changes and publish its findings so that the public could at least evaluate whether the companies were complying with the original orders. But the Commission remained silent, even as it claimed that its model was working well for these companies.

In 2012, EPIC sued the Commission when it became clear that Google was proposing to do precisely what the FTC said it could not – consolidate user data across various services that came with diverse privacy policies in order to build detailed individual profiles. The problem was widely understood. Many members of Congress in both parties, state attorneys general, and Jon Leibowitz, the head of the FTC itself, warned about the possible outcome. Even the federal court, which ruled that it could not require the agency to enforce its order, was sympathetic. "EPIC – along with many other individuals and organizations – has advanced serious concerns

<sup>26</sup> Letter from FTC Chairwoman Edith Ramirez to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission, at 4-5 (Jul. 7, 2016),

<https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015f00000004q0v>

<sup>27</sup> *In the Matter of Google, Inc.*, EPIC Complaint, Request for Investigation, Injunction, and Other Relief, before the Federal Trade Commission, Washington, D.C. (filed Feb. 16, 2010),

[https://epic.org/privacy/ftc/googlebuzz/GoogleBuzz\\_Complaint.pdf](https://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf); Fed. Trade Comm'n., *FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network: Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data*, Press Release, (Mar. 30, 2011), <https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz>.

that may well be legitimate, and the FTC, which has advised the Court that the matter is under review, may ultimately decide to institute an enforcement action," wrote the judge.<sup>28</sup>

But that enforcement action never came. Even afterward, EPIC and other consumer privacy organizations have continued to urge the Federal Trade Commission to enforce its consent orders. In our most recent comments to the Federal Trade Commissioner, we said simply "The FTC Must Enforce Existing Consent Orders." We wrote:

The effectiveness of FTC enforcement is determined by the agency's willingness to enforce the legal judgments it obtains. The FTC should review substantial changes in business practices for companies under consent orders that implicate the privacy interests of consumers. Multiple prominent internet firms have been permitted to alter business practices, without consequence, despite being subject to 20-year consent orders with the FTC. This has harmed consumers and promoted industry disregard for the FTC.<sup>29</sup>

The Committee should be specifically concerned about the FTC's ongoing failure to enforce its consent orders. This agency practice poses an ongoing risk to both American consumers and American businesses.

#### **Cambridge Analytica Breach**

On March 16, 2018, Facebook admitted the unlawful transfer of 50 million user profiles to the data mining firm Cambridge Analytica, which harvested the data obtained without consent to influence the 2016 U.S. presidential election.<sup>30</sup> Relying on the data provided by Facebook, Cambridge Analytica was able to collect the private information of approximately 270,000 users and their extensive friend networks under false pretenses as a research-driven application.<sup>31</sup> Last week, Facebook announced that the number of users who had their data unlawfully harvested was actually closer to 87 million.<sup>32</sup>

This is in clear violation of the 2011 Consent Order, which states that Facebook "shall not misrepresent in any manner, expressly or by implication ... the extent to which [Facebook] makes or has made covered information accessible to third parties; and the steps [Facebook] takes or has taken to verify the privacy or security protections that any third party provides."<sup>33</sup>

<sup>28</sup> *EPIC v. FTC*, 844 F. Supp. 2d 98 (D.D.C. 2012), <https://epic.org/privacy/ftc/google/EPICvFTCCtMemo.pdf>.

<sup>29</sup> EPIC Statement to FTC (Feb. 2017), <https://epic.org/privacy/internet/ftc/EPIC-et-al-ltr-FTC-02-15-2017.pdf>.

<sup>30</sup> Press Release, Facebook, *Suspending Cambridge Analytica and SCL Group from Facebook* (Mar. 16, 2018), <https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/>.

<sup>31</sup> *Id.*

<sup>32</sup> Cecilia Kang and Sheera Frenkel, *Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users*, N.Y. Times, (Apr. 4, 2018), <https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html>.

<sup>33</sup> Federal Trade Commission, *Facebook, Inc.; Analysis of Proposed Consent Order To Aid Public Comment*, 76 Fed. Reg. 75883 (Dec. 5, 2011),

Part II of the proposed order required Facebook to “give its users a clear and prominent notice and obtain their affirmative express consent before sharing their previously-collected information with third parties in any way that materially exceeds the restrictions imposed by their privacy settings.”<sup>34</sup> Part IV “requires Facebook to establish and maintain a comprehensive privacy program that is reasonably designed to: (1) Address privacy risks related to the development and management of new and existing products and services, and (2) protect the privacy and confidentiality of covered information. The privacy program must be documented in writing and must contain controls and procedures appropriate to Facebook’s size and complexity, the nature and scope of its activities, and the sensitivity of covered information.”<sup>35</sup>

**Response of EPIC and Consumer Privacy Organizations, Compliance with GDPR**

After the news broke of the Cambridge Analytica breach, EPIC and a consumer coalition urged the FTC to reopen the Facebook investigation.<sup>36</sup> We stated, “Facebook’s admission that it disclosed data to third parties without users’ consent suggests a clear violation of the 2011 Facebook Order.” We further said:

The FTC has an obligation to the American public to ensure that companies comply with existing Consent Orders. It is unconscionable that the FTC allowed this unprecedented disclosure of Americans’ personal data to occur. The FTC’s failure to act imperils not only privacy but democracy as well.

On March 26, 2018, less than two weeks ago, the FTC announced it would reopen the investigation.<sup>37</sup> The Statement by the Acting Director of FTC’s Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practice, issued on March 26, 2018, was as follows:

The FTC is firmly and fully committed to using all of its tools to protect the privacy of consumers. Foremost among these tools is enforcement action against companies that fail to honor their privacy promises, including to comply with Privacy Shield, or that engage in unfair acts that cause substantial injury to consumers in violation of the FTC Act. Companies who have settled previous

[https://www.ftc.gov/sites/default/files/documents/federal\\_register\\_notices/facebook-inc.analysis-proposed-consent-order-aid-public-comment-proposed-consent-agreement/111205facebookfn.pdf](https://www.ftc.gov/sites/default/files/documents/federal_register_notices/facebook-inc.analysis-proposed-consent-order-aid-public-comment-proposed-consent-agreement/111205facebookfn.pdf).

<sup>34</sup> *Id.* (emphasis added).

<sup>35</sup> *Id.* (emphasis added).

<sup>36</sup> Letter to Acting Chairman Maureen Ohlhausen and Commissioner Terrell McSweeney from leading consumer privacy organizations in the United States (Mar. 20, 2018), <https://epic.org/privacy/facebook/EPIC-et-al-ltr-FTC-Cambridge-FB-03-20-18.pdf>. See “EPIC, Consumer Groups Urge FTC To Investigate Facebook” (Mar. 20, 2018), <https://epic.org/2018/03/epic-consumer-groups-urge-ftc.html>.

<sup>37</sup> Fed. Trade Comm’n, *Statement by the Acting Director of FTC’s Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices* (March 26, 2018), <https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection>. See EPIC, “FTC Confirms Investigation into Facebook about 2011 Consent Order” (Mar. 26, 2018), <https://epic.org/2018/03/ftc-confirms-investigation-int.html>.

FTC actions must also comply with FTC order provisions imposing privacy and data security requirements. Accordingly, the FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook. Today, the FTC is confirming that it has an open non-public investigation into these practices.

Congress should monitor this matter closely. This may be one of the most consequential investigations currently underway in the federal government.

But others are not waiting for the resolution. State Attorneys General have also made clear their concerns about the Facebook matter.<sup>38</sup>

Also today, a broad coalition of consumer organizations in the United States and Europe, represented by the TransAtlantic Consumer Dialogue (“TACD”), will urge Mr. Zuckerberg to make clear his commitment to compliance with the General Data Protection Regulation. The TACD wrote:

The GDPR helps ensure that companies such as yours operate in an accountable and transparent manner, subject to the rule of law and the democratic process. The GDPR provides a solid foundation for data protection, establishing clear responsibilities for companies that collect personal data and clear rights for users whose data is gathered. These are protections that all users should be entitled to no matter where they are located.<sup>39</sup>

EPIC supports the recommendation of TACD concerning the GDPR. There is little reason that a U.S. firm should provide better privacy protection to individuals outside the United States than it does to those inside our country.

**Oversight of the Federal Trade Commission and Facebook Compliance with the 2011 Consent Order**

Several former FTC commissioners and former FTC staff members have recently suggested that the FTC needs more authority to protect American consumers. At least with regard to enforcement of its current legal authority, we strongly disagree. The FTC could have done far more than it did.

On March 20, 2018, EPIC submitted a request to the FTC under the Freedom of Information Act for the 2013, 2015, and 2017 Facebook Assessments, as well as all records concerning the person(s) approved by the FTC to undertake the Facebook Assessments; and all records of communications between the FTC and Facebook regarding the Facebook

<sup>38</sup> EPIC, “State AGs Launch Facebook Investigation,” (Mar. 26, 2018), <https://epic.org/2018/03/state-ags-launch-facebook-inve.html>.

<sup>39</sup> Letter from TACD to Mark Zuckerberg, CEO, Facebook, Inc., Apr. 9, 2018, [http://tacd.org/wp-content/uploads/2018/04/TACD-letter-to-Mark-Zuckerberg\\_final.pdf](http://tacd.org/wp-content/uploads/2018/04/TACD-letter-to-Mark-Zuckerberg_final.pdf).

Assessments. In 2013, EPIC received redacted version of Facebook's initial compliance report and first independent assessment after a similar FOIA request.<sup>40</sup>

Under the Final Consent Order, Facebook's initial assessment was due to the FTC on April 13, 2013, and the subsequent reporting deadlines were in 2015 and 2017. Cambridge Analytica engaged in the illicit collection of Facebook user data from 2014 to 2016, encompassed by the requested reporting period of the assessments.

We will keep the Committee informed of the progress of EPIC's FOIA request for the FTC reports on Facebook compliance. We also urge the Committee to pursue the public release of these documents. They will provide for you a fuller pictures of the FTC's lack of response to the looming privacy crisis in America.

### **Recommendations**

There is a lot of work ahead to safeguard the personal data of Americans. Here are a few preliminary recommendations:

- *Improve oversight of the Federal Trade Commission.* The FTC has failed to protect the privacy interests of American consumer and the Commission's inaction contributed directly to the Cambridge Analytica breach, and possibly the Brexit vote and the outcome of the 2016 Presidential election. Oversight of the Commission's failure to enforce the 2011 consent order is critical, particularly for the House Energy & Commerce Committee which also bears some responsibility for this outcome.
- *Update US privacy laws.* It goes without saying (though obviously it still needs to be said) that U.S. privacy law is out of date. There has always been a gap between changes in technology and business practices and the development of new privacy protections. But the gap today in the United States is the greatest at any time since the emergence of modern privacy law in the 1960s. The current approach is also unnecessarily inefficient, complex, and ineffective. And many of the current proposals, e.g. better privacy notices, would do little to protect privacy or address the problems arising from Cambridge Analytica debacle.
- *Establish a federal privacy agency in the United States.* The U.S. is one of the few developed countries in the world without a data protection agency. The practical consequence is that the U.S consumers experience the highest levels of data breach, financial fraud, and identity theft in the world. And U.S. businesses, with their vast collections of personal data, remain the target of cyber attack by criminals and foreign adversaries. The longer the U.S. continues on this course, the greater will be the threats to consumer privacy, democratic institutions, and national security.

<sup>40</sup> Facebook Initial Compliance Report (submitted to FTC on Nov. 13, 2012), <http://epic.org/foia/FTC/facebook/EPIC-13-04-26-FTC-FOIA-20130612-Production-1.pdf>; Facebook Initial Independent Assessment (submitted to FTC on Apr. 22, 2013), <http://epic.org/foia/FTC/facebook/EPIC-14-04-26-FTC-FOIA-20130612-Production-2.pdf>.

**Conclusion**

The transfer of 87 million user records to Cambridge Analytica could have been avoided if the FTC had done its job. The 2011 Consent Order against Facebook was issued to protect the privacy of user data. If it had been enforced, there would be no need for the hearing this week.

After the hearing with Mr. Zuckerberg this week, the Committee should ask current and former FTC Commissioners and key staff, “why didn’t you enforce the 2011 Consent Order against Facebook and prevent this mess?”<sup>41</sup>

We ask that this letter be submitted into the hearing record. EPIC looks forward to working with the Committee.

Sincerely,

/s/ Marc Rotenberg  
Marc Rotenberg  
EPIC President

/s/ Caitriona Fitzgerald  
Caitriona Fitzgerald  
EPIC Policy Director

/s/ Enid Zhou  
Enid Zhou  
EPIC Open Government Fellow

/s/ Sunny Kang  
Sunny Kang  
EPIC International Consumer Counsel

/s/ Sam Lester  
Sam Lester  
EPIC Consumer Privacy Fellow

**Attachment**

EPIC, *et al.* *In the Matter of Facebook, Inc: Complaint, Request for Investigation, Injunction, and Other Relief*, Before the Federal Trade Commission, Washington, DC (Dec. 17, 2009) (29 pages, 119 numbered paragraphs) (signatories include The Electronic Privacy Information Center, The American Library Association, The Center for Digital Democracy, The Consumer Federation of America, Patient Privacy Rights, Privacy Activism, Privacy Rights Now Coalition, The Privacy Rights Clearinghouse, The U.S. Bill of Rights Foundation).

<sup>41</sup> See Marc Rotenberg, *How the FTC Could Have Prevented the Facebook Mess*, *Techonomy* (Mar. 22, 2018), <https://techonomy.com/2018/03/how-the-ftc-could-have-avoided-the-facebook-mess/>.

Before the  
Federal Trade Commission  
Washington, DC

In the Matter of )  
 )  
Facebook, Inc. )  
 )  
\_\_\_\_\_ )

**Complaint, Request for Investigation, Injunction, and Other Relief**

I. Introduction

1. This complaint concerns material changes to privacy settings made by Facebook, the largest social network service in the United States, which adversely impact users of the Facebook service. Facebook’s changes to users’ privacy settings disclose personal information to the public that was previously restricted. Facebook’s changes to users’ privacy settings also disclose personal information to third parties that was previously not available. These changes violate user expectations, diminish user privacy, and contradict Facebook’s own representations. These business practices are Unfair and Deceptive Trade Practices, subject to review by the Federal Trade Commission (the “Commission”) under section 5 of the Federal Trade Commission Act.
2. These business practices impact more than 100 million users of the social networking site who fall within the jurisdiction of the United States Federal Trade Commission.<sup>1</sup>
3. EPIC urges the Commission to investigate Facebook, determine the extent of the harm to consumer privacy and safety, require Facebook to restore privacy settings that were previously available as detailed below, require Facebook to give users meaningful control over personal information, and seek appropriate injunctive and compensatory relief.

<sup>1</sup> Facebook, *Statistics*, <http://www.facebook.com/press/info.php?statistics> (last visited Dec. 14, 2009); see also Eric Eldon, *Facebook Reaches 100 Million Monthly Active Users in the United States*, InsideFacebook.com, Dec. 7, 2009, <http://www.insidefacebook.com/2009/12/07/facebook-reaches-100-million-monthly-active-users-in-the-united-states> (last visited Dec. 15, 2009).

II. Parties

4. The Electronic Privacy Information Center (“EPIC”) is a not-for-profit research center based in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the Federal Trade Commission. Among its other activities, EPIC first brought the Commission’s attention to the privacy risks of online advertising.<sup>2</sup> In 2004, EPIC filed a complaint with the FTC regarding the deceptive practices of data broker firm Choicepoint, calling the Commission’s attention to “data products circumvent[ing] the FCRA, giving businesses, private investigators, and law enforcement access to data that previously had been subjected to Fair Information Practices.”<sup>3</sup> As a result of the EPIC complaint, the FTC fined Choicepoint \$15 million.<sup>4</sup> EPIC initiated the complaint to the FTC regarding Microsoft Passport.<sup>5</sup> The Commission subsequently required Microsoft to implement a comprehensive information security program for Passport and similar services.<sup>6</sup> EPIC also filed a complaint with the FTC regarding the marketing of amateur spyware,<sup>7</sup> which resulted in the issuance of a permanent injunction barring sales of CyberSpy’s “stalker spyware,” over-the-counter surveillance technology sold for individuals to spy on other individuals.<sup>8</sup>

<sup>2</sup> *In the Matter of DoubleClick*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Feb. 10, 2000), available at [http://epic.org/privacy/internet/ftc/DCLK\\_complaint.pdf](http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf).

<sup>3</sup> *In the Matter of Choicepoint*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Dec. 16, 2004), available at <http://epic.org/privacy/choicepoint/feraltr12.16.04.html>.

<sup>4</sup> Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties*, \$5 Million for Consumer Redress, <http://www.ftc.gov/opa/2006/01/choicepoint.shtm> (last visited Dec. 13, 2009).

<sup>5</sup> *In the Matter of Microsoft Corporation*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (July 26, 2001), available at [http://epic.org/privacy/consumer/MS\\_complaint.pdf](http://epic.org/privacy/consumer/MS_complaint.pdf).

<sup>6</sup> *In the Matter of Microsoft Corporation*, File No. 012 3240, Docket No. C-4069 (Aug. 2002), available at <http://www.ftc.gov/os/caselist/0123240/0123240.shtm>. See also Fed. Trade Comm’n, “Microsoft Settles FTC Charges Alleging False Security and Privacy Promises” (Aug. 2002) (“The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years.”), available at <http://www.ftc.gov/opa/2002/08/microst.shtm>.

<sup>7</sup> *In the Matter of Awarenessstech.com, et al.*, Complaint and Request for Injunction, Request for Investigation and for Other relief, before the Federal Trade Commission, available at [http://epic.org/privacy/dv/spy\\_software.pdf](http://epic.org/privacy/dv/spy_software.pdf).

<sup>8</sup> *FTC v. Cyberspy Software*, No. 6:08-cv-1872 (D. Fla. Nov. 6, 2008) (unpublished order), available at <http://ftc.gov/os/caselist/0823160/081106cyberspytro.pdf>.



5. Earlier this year, EPIC urged the FTC to undertake an investigation of Google and cloud computing.<sup>9</sup> The FTC agreed to review the complaint, stating that it “raises a number of concerns about the privacy and security of information collected from consumers online.”<sup>10</sup> More recently, EPIC asked the FTC to investigate the “parental control” software firm Echometrix.<sup>11</sup> Thus far, the FTC has failed to announce any action in this matter, but once the Department of Defense became aware of the privacy and security risks to military families, it removed Echometrix’s software from the Army and Air Force Exchange Service, the online shopping portal for military families.<sup>12</sup>
6. The American Library Association is the oldest and largest library association in the world, with more than 64,000 members. Its mission is “to provide leadership for the development, promotion, and improvement of library and information services and the profession of librarianship in order to enhance learning and ensure access to information for all.”
7. The Center for Digital Democracy (“CDD”) is one of the leading non-profit groups analyzing and addressing the impact of digital marketing on privacy and consumer welfare. Based in Washington, D.C., CDD has played a key role promoting policy safeguards for interactive marketing and data collection, including at the FTC and Congress.
8. Consumer Federation of America (“CFA”) is an association of some 300 nonprofit consumer organizations across the U.S. CFA was created in 1968 to advance the consumer interest through research, advocacy, and education.
9. Patient Privacy Rights is a non-profit organization located in Austin, Texas. Founded in 2004 by Dr. Deborah Peel, Patient Privacy Rights is dedicated to ensuring Americans control all access to their health records.
10. Privacy Activism is a nonprofit organization whose goal is to enable people to make well-informed decisions about the importance of privacy on both a personal and societal

<sup>9</sup> *In the Matter of Google, Inc., and Cloud Computing Services*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Mar. 17, 2009), available at <http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf>.

<sup>10</sup> Letter from Eileen Harrington, Acting Director of the FTC Bureau of Consumer Protection, to EPIC (Mar. 18, 2009), available at [http://epic.org/privacy/cloudcomputing/google/031809\\_ftc\\_itr.pdf](http://epic.org/privacy/cloudcomputing/google/031809_ftc_itr.pdf).

<sup>11</sup> *In the Matter of Echometrix, Inc.*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Sep. 25, 2009), available at <http://epic.org/privacy/ftc/Echometrix%20FTC%20Complaint%20final.pdf>.

<sup>12</sup> EPIC, *Excerpts from Echometrix Documents*, [http://epic.org/privacy/echometrix/Excerpts\\_from\\_echometrix\\_docs\\_12-1-09.pdf](http://epic.org/privacy/echometrix/Excerpts_from_echometrix_docs_12-1-09.pdf) (last visited Dec. 13, 2009).

level. A key goal of the organization is to inform the public about the importance of privacy rights and the short- and long-term consequences of losing them, either inadvertently, or by explicitly trading them away for perceived or ill-understood notions of security and convenience.

11. The Privacy Rights Clearinghouse (“PRC”) is a nonprofit consumer organization with a two-part mission—consumer information and consumer advocacy. It was established in 1992 and is based in San Diego, CA. Among its several goals, PRC works to raise consumers’ awareness of how technology affects personal privacy and to empower consumers to take action to control their own personal information by providing practical tips on privacy protection.
12. The U. S. Bill of Rights Foundation is a non-partisan public interest law policy development and advocacy organization seeking remedies at law and public policy improvements on targeted issues that contravene the Bill of Rights and related Constitutional law. The Foundation implements strategies to combat violations of individual rights and civil liberties through Congressional and legal liaisons, coalition building, message development, project planning & preparation, tactical integration with supporting entities, and the filings of complaints and of *amicus curiae* briefs in litigated matters.
13. Facebook Inc. was founded in 2004 and is based in Palo Alto, California. Facebook’s headquarters are located at 156 University Avenue, Suite 300, Palo Alto, CA 94301. At all times material to this complaint, Facebook’s course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 45.

### III. The Importance of Privacy Protection

14. The right of privacy is a personal and fundamental right in the United States.<sup>13</sup> The privacy of an individual is directly implicated by the collection, use, and dissemination of personal information. The opportunities to secure employment, insurance, and credit, to obtain medical services and the rights of due process may be jeopardized by the misuse of personal information.<sup>14</sup>

<sup>13</sup> See *Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 763 (1989) (“both the common law and the literal understandings of privacy encompass the individual’s control of information concerning his or her person”); *Whalen v. Roe*, 429 U.S. 589, 605 (1977); *United States v. Katz*, 389 U.S. 347 (1967); *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

<sup>14</sup> Fed. Trade Comm’n, *Consumer Sentinel Network Data Book* 11 (2009) (charts describing how identity theft victims’ information have been misused).

15. The excessive collection of personal data in the United States coupled with inadequate legal and technological protections have led to a dramatic increase in the crime of identity theft.<sup>15</sup>
16. The federal government has established policies for privacy and data collection on federal web sites that acknowledge particular privacy concerns “when uses of web technology can track the activities of users over time and across different web sites” and has discouraged the use of such techniques by federal agencies.<sup>16</sup>
17. As the Supreme Court has made clear, and the Court of Appeals for the District of Columbia Circuit has recently held, “both the common law and the literal understanding of privacy encompass the individual’s control of information concerning his or her person.”<sup>17</sup>
18. The Organization for Economic Co-operation and Development (“OECD”) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data recognize that “the right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard.”
19. The appropriation tort recognizes the right of each person to protect the commercial value of that person’s name and likeness. The tort is recognized in virtually every state in the United States.
20. The Madrid Privacy Declaration of November 2009 affirms that privacy is a basic human right, notes that “corporations are acquiring vast amounts of personal data without independent oversight,” and highlights the critical role played by “Fair Information Practices that place obligations on those who collect and process personal information and gives rights to those whose personal information is collected.”<sup>18</sup>
21. The Federal Trade Commission is “empowered and directed” to investigate and prosecute violations of Section 5 of the Federal Trade Commission Act where the privacy interests of Internet users are at issue.<sup>19</sup>

<sup>15</sup> *Id.* at 5 (from 2000-2009, the number of identity theft complaints received increased from 31,140 to 313,982); see U.S. Gen. Accounting Office, *Identity Theft: Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain* 8 (2009); Fed. Trade Comm’n, *Security in Numbers: SSNs and ID Theft 2* (2008).

<sup>16</sup> Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies* (2000), available at [http://www.whitehouse.gov/omb/memoranda\\_m00-13](http://www.whitehouse.gov/omb/memoranda_m00-13) (last visited Dec. 17, 2009).

<sup>17</sup> *U.S. Dep’t of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989), cited in *Nat’l Cable & Tele. Assn. v. Fed. Commc’ns. Comm’n*, No. 07-1312 (D.C. Cir. Feb. 13, 2009).

<sup>18</sup> The Madrid Privacy Declaration: Global Privacy Standards for a Global World, Nov. 3, 2009, available at <http://thepublicvoice.org/madrid-declaration/>.

<sup>19</sup> 15 U.S.C. § 45 (2006).

IV. Factual Background**Facebook's Size and Reach Is Unparalleled Among Social Networking Sites**

22. Facebook is the largest social network service provider in the United States. According to Facebook, there are more than 350 million active users, with more than 100 million in the United States. More than 35 million users update their statuses at least once each day.<sup>20</sup>
23. More than 2.5 billion photos are uploaded to the site each month.<sup>21</sup> Facebook is the largest photo-sharing site on the internet, by a wide margin.<sup>22</sup>
24. As of August 2009, Facebook is the fourth most-visited web site in the world, and the sixth most-visited web site in the United States.<sup>23</sup>

**Facebook Has Previously Changed Its Service in Ways that Harm Users' Privacy**

25. In September 2006, Facebook disclosed users' personal information, including details relating to their marital and dating status, without their knowledge or consent through its "News Feed" program.<sup>24</sup> Hundreds of thousands of users objected to Facebook's actions.<sup>25</sup> In response, Facebook stated:

We really messed this one up. When we launched News Feed and Mini-Feed we were trying to provide you with a stream of information about your social world. Instead, we did a bad job of explaining what the new features were and an even worse job of giving you control of them.<sup>26</sup>

26. In 2007, Facebook disclosed users' personal information, including their online purchases and video rentals, without their knowledge or consent through its "Beacon" program.<sup>27</sup>
27. Facebook is a defendant in multiple federal lawsuits<sup>28</sup> arising from the "Beacon" program.<sup>29</sup> In the lawsuits, users allege violations of federal and state law, including the

<sup>20</sup> Facebook, *Statistics*, <http://www.facebook.com/press/info.php?statistics> (last visited Dec. 14, 2009).

<sup>21</sup> *Id.*

<sup>22</sup> Erick Schonfeld, *Facebook Photos Pulls Away From the Pack*, TechCrunch (Feb. 22, 2009), <http://www.techcrunch.com/2009/02/22/facebook-photos-pulls-away-from-the-pack/>.

<sup>23</sup> Erick Schonfeld, *Facebook is Now the Fourth Largest Site in the World*, TechCrunch (Aug. 4, 2009), <http://www.techcrunch.com/2009/08/04/facebook-is-now-the-fourth-largest-site-in-the-world/>.

<sup>24</sup> See generally EPIC, *Facebook Privacy*, <http://epic.org/privacy/facebook/> (last visited Dec. 15, 2009).

<sup>25</sup> Justin Smith, *Scared students protest Facebook's social dashboard, grappling with rules of attention economy*, Inside Facebook (Sept. 6, 2006), <http://www.insidefacebook.com/2006/09/06/scared-students-protest-facebooks-social-dashboard-grappling-with-rules-of-attention-economy/>.

<sup>26</sup> Mark Zuckerberg, *An Open Letter from Mark Zuckerberg* (Sept. 8, 2006), <http://blog.facebook.com/blog.php?post=2208562130>.

<sup>27</sup> See generally EPIC, *Facebook Privacy*, <http://epic.org/privacy/facebook/> (last visited Dec. 15, 2009).

Video Privacy Protection Act, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and California's Computer Crime Law.<sup>30</sup>

28. On May 30, 2008, the Canadian Internet Policy and Public Interest Clinic filed a complaint with Privacy Commissioner of Canada concerning the "unnecessary and non-consensual collection and use of personal information by Facebook."<sup>31</sup>
29. On July 16, 2009, the Privacy Commissioner's Office found Facebook "in contravention" of Canada's Personal Information Protection and Electronic Documents Act.<sup>32</sup>
30. The Privacy Commissioner's Office found:
 

Facebook did not have adequate safeguards in place to prevent unauthorized access by application developers to users' personal information, and furthermore was not doing enough to ensure that meaningful consent was obtained from individuals for the disclosure of their personal information to application developers.<sup>33</sup>
31. On February 4, 2009, Facebook revised its Terms of Service, asserting broad, permanent, and retroactive rights to users' personal information—even after they deleted their accounts.<sup>34</sup> Facebook stated that it could make public a user's "name, likeness and image for any purpose, including commercial or advertising."<sup>35</sup>
32. Users objected to Facebook's actions, and Facebook reversed the revisions on the eve of an EPIC complaint to the Commission.<sup>36</sup>

---

<sup>28</sup> In *Lane v. Facebook, Inc.*, No. 5:08-CV-03845 (N.D. Cal. filed Aug. 12, 2008), Facebook has requested court approval of a class action settlement that would terminate users' claims, but provide no monetary compensation to users. The court has not ruled on the matter.

<sup>29</sup> See e.g., *Harris v. Facebook, Inc.*, No. 09-01912 (N.D. Tex. filed Oct. 9, 2009); *Lane v. Facebook, Inc.*, No. 5:08-CV-03845 (N.D. Cal. filed Aug. 12, 2008); see also *Harris v. Blockbuster*, No. 09-217 (N.D. Tex. filed Feb. 3, 2009), *appeal docketed*, No. 09-10420 (5th Cir. Apr. 29, 2009).

<sup>30</sup> *Id.*

<sup>31</sup> Letter from Philippa Lawson, Director, Canadian Internet Policy and Public Interest Clinic to Jennifer Stoddart, Privacy Commissioner of Canada (May 30, 2008), available at [http://www.cippic.ca/uploads/CIPPICFacebookComplaint\\_29May08.pdf](http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf).

<sup>32</sup> Elizabeth Denham, Assistant Privacy Commissioner of Canada, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*, July 16, 2009, available at [http://priv.gc.ca/cf-dc/2009/2009\\_008\\_0716\\_e.pdf](http://priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf).

<sup>33</sup> *Id.* at 3.

<sup>34</sup> Chris Walters, *Facebook's New Terms Of Service: "We Can Do Anything We Want With Your Content. Forever."* The Consumerist, Feb. 15, 2009, available at <http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html#reset>.

<sup>35</sup> *Id.*

<sup>36</sup> JR Raphael, *Facebook's Privacy Flap: What Really Went Down, and What's Next*, PC World, Feb. 18, 2009, [http://www.pcworld.com/article/159743/facebooks\\_privacy\\_flap\\_what\\_really\\_went\\_down\\_and\\_whats\\_next.html](http://www.pcworld.com/article/159743/facebooks_privacy_flap_what_really_went_down_and_whats_next.html).

**Changes in Privacy Settings: “Publicly Available Information”**

33. Facebook updated its privacy policy and changed the privacy settings available to users on November 19, 2009 and again on December 9, 2009.<sup>37</sup>
34. Facebook now treats the following categories of personal data as “publicly available information:”
- users’ names,
  - profile photos,
  - lists of friends,
  - pages they are fans of,
  - gender,
  - geographic regions, and
  - networks to which they belong.<sup>38</sup>
35. By default, Facebook discloses “publicly available information” to search engines, to Internet users whether or not they use Facebook, and others. According to Facebook, such information can be accessed by “every application and website, including those you have not connected with . . . .”<sup>39</sup>
36. Prior to these changes, only the following items were mandatorily “publicly available information:”
- a user’s name and
  - a user’s network.

<sup>37</sup> Facebook, *Facebook Asks More Than 350 Million Users Around the World To Personalize Their Privacy* (Dec. 9, 2009), available at <http://www.facebook.com/press/releases.php?p=133917>.

<sup>38</sup> Facebook, *Privacy Policy*, <http://www.facebook.com/policy.php> (last visited Dec. 16, 2009).

<sup>39</sup> *Id.*

37. Users also had the option to include additional information in their public search listing, as the screenshot of the original privacy settings for search discovery demonstrates.

**Privacy > Search**

**Search Discovery**  
Use this setting below to control who on Facebook can find you through search. Your Friends will always be able to find you.

Search Visibility: Everyone

**Search Result Content**  
People who can find you in search can click through to a very limited version of your profile. Use these checkboxes to control what people can see in addition to your name.

People who can see me in search can see:

- My profile picture
- My friend list
- A link to add me as a friend
- A link to send me a message
- Pages I am a fan of

**Public Search Listing**  
Use this setting to control whether your search result is available outside of Facebook.

Create a public search listing for me and submit it for search engine indexing (see preview)

Please note that minors do not have public search listings - listings created by minors will activate only when they are no longer minors.

38. Facebook's original privacy policy stated that users "may not want everyone in the world to have the information you share on Facebook" as the screenshot below makes clear:

**Facebook Principles**

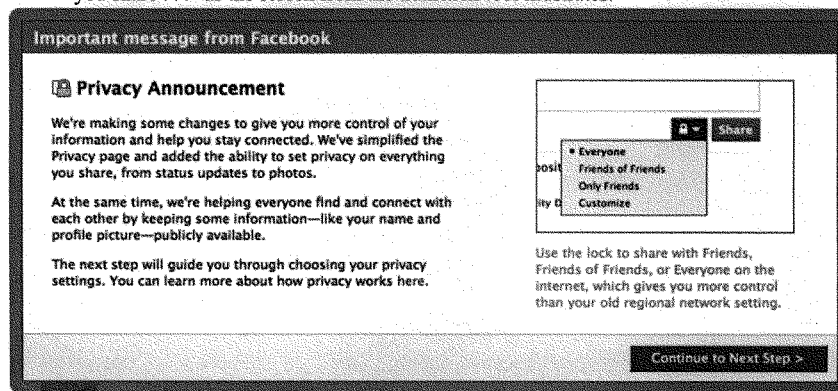
We built Facebook to make it easy to share information with your friends and people around you. We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your networks and other reasonable community limitations that we tell you about.

Facebook follows two core principles:

- 1. You should have control over your personal information.**  
Facebook helps you share information with your friends and people around you. You choose what information you put in your profile, including contact and personal information, pictures, interests and groups you join. And you control the users with whom you share that information through the privacy settings on the Privacy page.
- 2. You should have access to the information others want to share.**  
There is an increasing amount of information available out there, and you may want to know what relates to you, your friends, and people around you. We want to help you easily get that information.

Sharing information should be easy. And we want to provide you with the privacy tools necessary to control how and with whom you share that information. If you have questions or ideas, please send them to [privacy@facebook.com](mailto:privacy@facebook.com).

39. Facebook's Chief Privacy Officer, Chris Kelly, testified before Congress that Facebook gives "users controls over how they share their personal information that model real-world information sharing and provide them transparency about how we use their information in advertising."<sup>40</sup> Kelly further testified, "many of our users choose to limit what profile information is available to non-friends. Users have extensive and precise controls available to choose who sees what among their networks and friends, as well as tools that give them the *choice* to make a limited set of information available to search engines and other outside entities."<sup>41</sup>
40. In an "Important message from Facebook," Facebook told users it was giving "you more control of your information . . . and [had] added the ability to set privacy on everything you share . . ." as the screen from the transition tool illustrates:



41. Facebook's CEO, Mark Zuckerberg, reversed changes to his personal Facebook privacy settings after the transition from the original privacy settings to the revised settings made public his photographs and other information.<sup>42</sup>
42. Barry Schnitt, Facebook's Director of Corporate Communications and Public Policy, "suggests that users are free to lie about their hometown or take down their profile picture to protect their privacy."<sup>43</sup>

<sup>40</sup> Testimony of Chris Kelly, Chief Privacy Officer, Facebook, Before the U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection Subcommittee on Communications, Technology and the Internet (June 18, 2009), available at [http://energycommerce.house.gov/Press\\_111/20090618/testimony\\_kelly.pdf](http://energycommerce.house.gov/Press_111/20090618/testimony_kelly.pdf).

<sup>41</sup> *Id.*

<sup>42</sup> Kashmir Hill, *Either Mark Zuckerberg got a whole lot less private or Facebook's CEO doesn't understand the company's new privacy settings* (Dec. 10, 2009), <http://trueslant.com/KashmirHill/2009/12/10/either-mark-zuckerberg-got-a-whole-lot-less-private-or-facebooks-ceo-doesnt-understand-the-companys-new-privacy-settings/>.



43. Providing false information on a Facebook profile violates Facebook's Terms of Service.<sup>44</sup>
44. Facebook user profile information may include sensitive personal information.
45. Facebook users can indicate that they are "fans" of various organizations, individuals, and products, including controversial political causes.<sup>45</sup>
46. Under the original privacy settings, users controlled public access to the causes they supported. Under the revised settings, Facebook has made users' causes "publicly available information," disclosing this data to others and preventing users from exercising control as they had under the original privacy policy.
47. Based on profile data obtained from Facebook users' friends lists, MIT researchers found that "just by looking at a person's online friends, they could predict whether the person was gay."<sup>46</sup> Under Facebook's original privacy policy, Facebook did not categorize users' friends lists as "publicly available information." Facebook now makes users' friends lists "publicly available information."
48. Dozens of American Facebook users, who posted political messages critical of Iran, have reported that Iranian authorities subsequently questioned and detained their relatives.<sup>47</sup> Under the revised privacy settings, Facebook makes such users' friends lists publicly available.

---

<sup>43</sup> Julia Angwin, *How Facebook Is Making Friending Obsolete*, Wall St. J., Dec. 15, 2009, available at <http://online.wsj.com/article/SB126084637203791583.html>.

<sup>44</sup> Facebook, Statement of Rights and Responsibilities, <http://www.facebook.com/terms.php> (last visited Dec. 16, 2009); see Jason Kincaid, *Facebook Suggests You Lie, Break Its Own Terms Of Service To Keep Your Privacy*, Washington Post, Dec. 16, 2009, available at <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/15/AR2009121505270.html>.

<sup>45</sup> See, e.g., Facebook, *Prop 8*, <http://www.facebook.com/pages/Prop-8/86610985605> (last visited Dec. 15, 2009); Facebook, *No on Prop 8 Don't Eliminate Marriage for Anyone*, <http://www.facebook.com/#/pages/No-on-Prop-8-Dont-Eliminate-Marriage-for-Anyone/29097894014> (last visited Dec. 15, 2009); see also *Court Tosses Prop. 8 Ruling on Strategy Papers*, San Francisco Chron. (Dec. 12, 2009), available at <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/12/11/BA3A1B34VC.DTL>.

<sup>46</sup> See Carolyn Y. Johnson, *Project "Gaydar"*, Sep. 20, 2009, Boston Globe, available at [http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project\\_gaydar\\_an\\_mit\\_experiment\\_raises\\_new\\_questions\\_about\\_online\\_privacy/?page=full](http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/?page=full)

<sup>47</sup> Farnaz Fasshi, *Iranian Crackdown Goes Global*, Wall Street Journal (Dec. 4, 2009), available at <http://online.wsj.com/article/SB125978649644673331.html>.

49. According to the Wall Street Journal, one Iranian-American graduate student received a threatening email that read, “we know your home address in Los Angeles,” and directed the user to “stop spreading lies about Iran on Facebook.”<sup>48</sup>
50. Another U.S. Facebook user who criticized Iran on Facebook stated that security agents in Tehran located and arrested his father as a result of the postings.<sup>49</sup>
51. One Facebook user who traveled to Iran said that security officials asked him whether he owned a Facebook account, and to verify his answer, they performed a Google search for his name, which revealed his Facebook page. His passport was subsequently confiscated for one month, pending interrogation.<sup>50</sup>
52. Many Iranian Facebook users, out of fear for the safety of their family and friends, changed their last name to “Irani” on their pages so government officials would have a more difficult time targeting them and their loved ones.<sup>51</sup>
53. By implementing the revised privacy settings, Facebook discloses users’ sensitive friends lists to the public and exposes users to the analysis employed by Iranian officials against political opponents.

**Changes to Privacy Settings: Information Disclosure to Application Developers**

54. The Facebook Platform transfers Facebook users’ personal data to application developers without users’ knowledge or consent.<sup>52</sup>
55. Facebook permits third-party applications to access user information at the moment a user visits an application website. According to Facebook, third party applications receive publicly available information automatically when you visit them, and additional information when you formally authorize or connect your Facebook account with them.<sup>53</sup>
56. As Facebook itself explains in its documentation, when a user adds an application, by default that application then gains access to everything on Facebook that the user can

---

<sup>48</sup> *Id.*

<sup>49</sup> *Id.*

<sup>50</sup> *Id.*

<sup>51</sup> *Id.*

<sup>52</sup> See Facebook, *Facebook Platform*, <http://www.facebook.com/facebook#/platform?v=info> (last visited Dec. 13, 2009).

<sup>53</sup> Facebook, *Privacy Policy*, <http://www.facebook.com/policy.php> (last visited Dec. 16, 2009).

sec.<sup>54</sup> The primary “privacy setting” that Facebook demonstrates to third-party developers governs what other users can see from the application’s output, rather than what data may be accessed by the application.<sup>55</sup>

57. According to Facebook:

Examples of the types of information that applications and websites may have access to include the following information, to the extent visible on Facebook: your name, your profile picture, your gender, your birthday, your hometown location (city/state/country), your current location (city/state/country), your political view, your activities, your interests, your musical preferences, television shows in which you are interested, movies in which you are interested, books in which you are interested, your favorite quotes, your relationship status, your dating interests, your relationship interests, your network affiliations, your education history, your work history, your course information, copies of photos in your photo albums, metadata associated with your photo albums (e.g., time of upload, album name, comments on your photos, etc.), the total number of messages sent and/or received by you, the total number of unread messages in your in-box, the total number of “pokes” you have sent and/or received, the total number of wall posts on your Wall, a list of user IDs mapped to your friends, your social timeline, notifications that you have received from other applications, and events associated with your profile.<sup>56</sup>

58. To access this information, developers use the Facebook Application Programming Interface (“API”), to “utiliz[e] profile, friend, Page, group, photo, and event data.”<sup>57</sup> The API is a collection of commands that an application can run on Facebook, including authorization commands, data retrieval commands, and data publishing commands.<sup>58</sup>

<sup>54</sup> Facebook, *About Platform*, [http://developers.facebook.com/about\\_platform.php](http://developers.facebook.com/about_platform.php) (last visited Dec. 16, 2009).

<sup>55</sup> Facebook Developer Wiki, *Anatomy of a Facebook App*, [http://wiki.developers.facebook.com/index.php/Anatomy\\_of\\_a\\_Facebook\\_App#Privacy\\_Settings](http://wiki.developers.facebook.com/index.php/Anatomy_of_a_Facebook_App#Privacy_Settings) (last visited Dec. 16, 2009).

<sup>56</sup> Facebook, *About Platform*, [http://developers.facebook.com/about\\_platform.php](http://developers.facebook.com/about_platform.php) (last visited Dec. 16, 2009).

<sup>57</sup> Facebook Developer Wiki, *API*, <http://wiki.developers.facebook.com/index.php/API> (last visited Dec. 16, 2009).

<sup>58</sup> *Id.*

59. Third-parties who develop Facebook applications may also transmit the user information they access to their own servers, and are asked only to retain the information for less than 24 hours.<sup>59</sup>
60. A 2007 University of Virginia study of Facebook applications found that “90.7% of applications are being given more privileges than they need.”<sup>60</sup>
61. According to the Washington Post, many Facebook developers who have gained access to information this way have considered the “value” of having the data, even when the data is not relevant to the purpose for which the user has added the application.<sup>61</sup>
62. Under the revised privacy policy, Facebook now categorizes users’ names, profile photos, lists of friends, pages they are fans of, gender, geographic regions, and networks to which they belong as “publicly available information,” and Facebook sets the “default privacy setting for certain types of information [users] post on Facebook . . . to ‘everyone.’”<sup>62</sup>
63. Facebook allows user information that is categorized as publicly available to “everyone” to be: “accessed by everyone on the Internet (including people not logged into Facebook);” made subject to “indexing by third party search engines;” “associated with you outside of Facebook (such as when you visit other sites on the internet);” and “imported and exported by us and others *without* privacy limitations.”<sup>63</sup>
64. With the Preferred Developer Program, Facebook will give third-party developers access to a user’s primary email address, personal information provided by the user to Facebook to subscribe to the Facebook service, but not necessarily available to the public or to developers.<sup>64</sup> In fact, some users may choose to create a Facebook account precisely to prevent the disclosure of their primary email address.

<sup>59</sup> Facebook Developer Wiki, *Policy Examples and Explanations/Data and Privacy*, [http://wiki.developers.facebook.com/index.php/Policy\\_Examples\\_and\\_Explanations/Data\\_and\\_Privacy](http://wiki.developers.facebook.com/index.php/Policy_Examples_and_Explanations/Data_and_Privacy) (last visited Dec. 16, 2009).

<sup>60</sup> Adrienne Felt & David Evans, *Privacy Protection for Social Networking APIs*, <http://www.cs.virginia.edu/felt/privacy/> (last visited Dec. 16, 2009).

<sup>61</sup> Kim Hart, *A Flashy Facebook Page, at a Cost to Privacy*, Wash. Post, June 12, 2008, available at <http://www.washingtonpost.com/wp-dyn/content/article/2008/06/11/AR2008061103759.html>

<sup>62</sup> Facebook, *Privacy Policy*, <http://www.facebook.com/policy.php> (last visited Dec. 16, 2009).

<sup>63</sup> *Id.* (emphasis added)

<sup>64</sup> Facebook, *Developer Roadmap*, [http://wiki.developers.facebook.com/index.php/Developer\\_Roadmap](http://wiki.developers.facebook.com/index.php/Developer_Roadmap) (last visited Dec. 17 2009); Facebook, *Roadmap Email*, [http://wiki.developers.facebook.com/index.php/Roadmap\\_Email](http://wiki.developers.facebook.com/index.php/Roadmap_Email) (last visited Dec. 17, 2009); see also Mark Walsh, *Facebook Starts Preferred Developer Program* (Dec. 17, 2009), [http://www.mediapost.com/publications/?fa=Articles.showArticle&art\\_aid=119293](http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=119293).

65. Facebook states in the revised privacy policy that users can “opt-out of Facebook Platform and Facebook Connect altogether through [their] privacy settings.”<sup>65</sup> Facebook further states that, “you can control how you share information with those third-party applications and websites through your application settings.”<sup>66</sup>

66. In fact, under the original privacy settings, users had a one-click option to prevent the disclosure of personal information to third party application developers through the Facebook API, as the screenshot below indicates:

Do not share any information about me through the Facebook API

67. Under the revised privacy settings, Facebook has eliminated the universal one-click option and replaced it with the screen illustrated below.<sup>67</sup>

Privacy Settings > Applications and Websites

**Applications and Websites**

**What your friends can share about you through applications and websites**

When your friend visits a Facebook-enhanced application or website, they may want to share certain information to make the experience more social. For example, a greeting card application may use your birthday information to prompt your friend to send a card.

If your friend uses an application that you do not use, you can control what types of information the application can access. Please note that applications will always be able to access your publicly available information (Name, Profile Picture, Gender, Current City, Networks, Friend List, and Pages) and information that is visible to Everyone.

- Personal info (activities, interests, etc.)
- Status updates
- Online presence
- Website
- Family and relationship
- Education and work
- My videos
- My links
- My notes
- My photos
- Photos and videos of me
- About me
- My birthday
- My hometown
- My religious and political views

<sup>65</sup> Facebook, *Privacy Policy*, <http://www.facebook.com/policy.php> (last visited Dec. 16, 2009).

<sup>66</sup> *Id.*

<sup>67</sup> Facebook, *Privacy Settings*, [http://www.facebook.com/settings/?tab=privacy&section=applications&field=friends\\_share](http://www.facebook.com/settings/?tab=privacy&section=applications&field=friends_share) (last visited Dec. 13, 2009).

68. Under the revised settings, even when a user unchecks all boxes and indicates that none of the personal information listed above should be disclosed to third party application developers, Facebook states that “applications will *always* be able to access your publicly available information (Name, Profile Picture, Gender, Current City, Networks, Friend List, and Pages) and information that is visible to Everyone.”<sup>68</sup>
69. Facebook’s “Everyone” setting overrides the user’s choice to limit access by third-party applications and websites.
70. Facebook does not now provide the option that explicitly allows users to opt out of disclosing all information to third parties through the Facebook Platform.
71. Users can block individual third-party applications from obtaining personal information by searching the Application Directory, visiting the application’s “about” page, clicking a small link on that page, and then confirming their decision.<sup>69</sup> A user would have to perform these steps for each of more than 350,000 applications in order to block all of them.<sup>70</sup>

#### **Facebook Users Oppose the Changes to the Privacy Settings**

72. Facebook users oppose these changes. In only four days, the number of Facebook groups related to privacy settings grew to more than five hundred.<sup>71</sup> Many security experts, bloggers, consumer groups, and news organizations have also opposed these changes.
73. More than 1,050 Facebook users are members of a group entitled “Against The New Facebook Privacy Settings!” The group has a simple request: “We demand that Facebook stop forcing people to reveal things they don’t feel comfortable revealing.”<sup>72</sup>
74. More than 950 Facebook users are members of a group entitled “Facebook! Fix the Privacy Settings,” which exhorts users to “tell Facebook that our personal information is private, and we want to control it!”<sup>73</sup>

<sup>68</sup> *Id.* (emphasis added)

<sup>69</sup> Facebook, *General Application Support: Application Safety and Security*, <http://www.facebook.com/help.php?page=967> (last visited Dec. 14, 2009).

<sup>70</sup> Facebook, *Statistics*, <http://www.facebook.com/press/info.php?statistics> (last visited Dec. 14, 2009).

<sup>71</sup> Facebook, *Search “privacy settings,”*

<http://www.facebook.com/search/?o=69&init=s%3Agroup&q=privacy%20settings> (last visited Dec. 15, 2009).

<sup>72</sup> Facebook, *Against The New Facebook Privacy Settings!*, <http://www.facebook.com/group.php?gid=209833062912> (last visited Dec. 15, 2009).

75. More than 74,000 Facebook users are members of a group entitled “Petition: Facebook, stop invading my privacy!”<sup>74</sup> The group objects to the revisions and hopes to “get a message across to Facebook.”<sup>75</sup> The group description explains, “[o]n December 9, 2009 Facebook once again breached our privacy by imposing new ‘privacy settings’ on 365+ million users. These settings notably give us LESS privacy than we had before, so I ask, how exactly do they make us more secure? . . . Perhaps the most frustrating and troublesome part is the changes Facebook made on our behalf without truly making us aware or even asking us.”<sup>76</sup>
76. A Facebook blog post discussing the changes to Facebook’s privacy policy and settings drew 2,000 comments from users, most of them critical of the changes.<sup>77</sup> One commenter noted, “I came here to communicate with people with whom I have some direct personal connection; not to have my personal information provided to unscrupulous third party vendors and made available to potential stalkers and identity thieves.”<sup>78</sup> Another commented, “I liked the old privacy settings better. I felt safer and felt like I had more control.”<sup>79</sup>
77. The Electronic Frontier Foundation posted commentary online discussing the “good, the bad, and the ugly” aspects of Facebook’s revised privacy policy and settings. More than 400 people have “tweeted” this article to encourage Facebook users to read EFF’s analysis.<sup>80</sup>
78. The American Civil Liberties Union of Northern California’s Demand Your dotRights campaign started a petition to Facebook demanding that Facebook (1) give full control of user information back to users; (2) give users strong default privacy settings; and (3) restrict the access of third party applications to user data.<sup>81</sup> The ACLU is “concerned that

---

<sup>73</sup> Facebook, *Facebook! Fix the Privacy Settings*, <http://www.facebook.com/group.php?gid=192282128398> (last visited Dec. 15, 2009).

<sup>74</sup> Facebook, *Petition: Facebook, stop invading my privacy!*, <http://www.facebook.com/group.php?gid=5930262681&ref=share> (last visited Dec. 15, 2009).

<sup>75</sup> *Id.*

<sup>76</sup> *Id.*

<sup>77</sup> See The Facebook Blog, *Updates on Your New Privacy Tools*, <http://blog.facebook.com/blog.php?post=197943902130> (last visited Dec. 14, 2009).

<sup>78</sup> *Id.*

<sup>79</sup> *Id.*

<sup>80</sup> See Twitter, *Twitter Search “eff.org Facebook,”* <http://twitter.com/#search?q=eff.org%20facebook> (last visited Dec. 14, 2009).

<sup>81</sup> American Civil Liberties Union, *Demand Your dotRights: Facebook Petition*, [https://secure.aclu.org/site/SPageNavigator/CN\\_Facebook\\_Privacy\\_Petition](https://secure.aclu.org/site/SPageNavigator/CN_Facebook_Privacy_Petition) (last visited Dec. 15, 2009).

the changes Facebook has made actually remove some privacy controls and encourage Facebook users to make other privacy protections disappear.”<sup>82</sup>

79. In the past week, more than 3,000 blog posts have been written focusing on criticism of Facebook’s privacy changes.<sup>83</sup>

80. After rolling out the revised Facebook privacy settings, widespread user criticism of the change in the “view friends” setting prompted Facebook to roll back the changes in part: “In response to your feedback, we’ve improved the Friend List visibility option described below. Now when you uncheck the ‘Show my friends on my profile’ option in the Friends box on your profile, your Friend List won’t appear on your profile regardless of whether people are viewing it while logged into Facebook or logged out.” Facebook further stated that “this information is still publicly available, however, and can be accessed by applications.”<sup>84</sup>

81. Ed Felten, a security expert and Princeton University professor,<sup>85</sup> stated:

As a user myself, I was pretty unhappy about the recently changed privacy control. I felt that Facebook was trying to trick me into loosening controls on my information. Though the initial letter from Facebook founder Mark Zuckerberg painted the changes as pro-privacy ... the actual effect of the company’s suggested new policy was to allow more public access to information. Though the company has backtracked on some of the changes, problems remain.<sup>86</sup>

82. Joseph Bonneau, a security expert and University of Cambridge researcher, criticized Facebook’s disclosure of users’ friend lists, observing,

there have been many research papers, including a few by me and colleagues in Cambridge, concluding that [friend lists are] actually the most important information to keep private. The threats here are more

<sup>82</sup> *Id.*, see also ACLUNC dotRights, *What Does Facebook’s Privacy Transition Mean for You?*, <http://dotrights.org/what-does-facebooks-privacy-transition-mean-you> (last visited Dec. 16, 2009).

<sup>83</sup> See Google, *Google Blog Search “facebook privacy criticism,”* [http://blogsearch.google.com/blogsearch?client=news&hl=en&q=facebook+privacy+criticism&ie=UTF-8&as\\_drrb=q&as\\_qdr=w](http://blogsearch.google.com/blogsearch?client=news&hl=en&q=facebook+privacy+criticism&ie=UTF-8&as_drrb=q&as_qdr=w) (last visited Dec. 14, 2009).

<sup>84</sup> The Facebook Blog, *Updates on Your New Privacy Tools*, <http://blog.facebook.com/blog.php?post=197943902130> (last visited Dec. 14, 2009).

<sup>85</sup> Prof. Felten is also Director of the Princeton Center for Information Technology Policy, a cross-disciplinary effort studying digital technologies in public life.

<sup>86</sup> Ed Felten, *Another Privacy Misstep from Facebook* (Dec. 14, 2009), <http://www.freedom-to-tinker.com/blog/felten/another-privacy-misstep-facebook>.



fundamental and dangerous-unexpected inference of sensitive information, cross-network de-anonymisation, socially targeted phishing and scams.<sup>87</sup>

Bonneau predicts that Facebook “will likely be completely crawled fairly soon by professional data aggregators, and probably by enterprising researchers soon after.”<sup>88</sup>

83. Security expert<sup>89</sup> Graham Cluley stated:

if you make your information available to “everyone,” it actually means “everyone, forever.” Because even if you change your mind, it's too late - and although Facebook say they will remove it from your profile they will have no control about how it is used outside of Facebook.

Cluley further states, “there's a real danger that people will go along with Facebook's recommendations without considering carefully the possible consequences.”<sup>90</sup>

84. Other industry experts anticipated the problems that would result from the changes in Facebook's privacy settings. In early July, TechCrunch, Jason Kincaid wrote:

Facebook clearly wants its users to become more comfortable sharing their content across the web, because that's what needs to happen if the site is going to take Twitter head-on with real-time search capabilities. Unfortunately that's far easier said than done for the social network, which has for years trumpeted its granular privacy settings as one of its greatest assets.<sup>91</sup>

Kincaid observed that “Facebook sees its redesigned control panel as an opportunity to invite users to start shrugging off their privacy. So it's piggybacking the new ‘Everyone’ feature on top of the Transition Tool . . .”<sup>92</sup>

<sup>87</sup> Joseph Bonneau, *Facebook Tosses Graph Privacy into the Bin* (Dec. 11, 2009), <http://www.lightbluetouchpaper.org/2009/12/11/facebook-tosses-graph-privacy-into-the-bin/>; see also Arvind Narayanan and Vitaly Shmatikov, *De-Anonymizing Social Networks*, available at <http://www.scribd.com/doc/15021482/DeAnonymizing-Social-Networks-Shmatikov-Narayanan>; *Phishing Attacks Using Social Networks*, <http://www.indiana.edu/~phishing/social-network-experiment/> (last visited Dec. 15, 2009).

<sup>88</sup> Bonneau, *Facebook Tosses Graph Privacy into the Bin*.

<sup>89</sup> Wikipedia, *Graham Cluley*, [http://en.wikipedia.org/wiki/Graham\\_Cluley](http://en.wikipedia.org/wiki/Graham_Cluley).

<sup>90</sup> Graham Cluley, *Facebook privacy settings: What you need to know* (Dec. 10, 2009) <http://www.sophos.com/blogs/gc/g/2009/12/10/facebook-privacy/>.

<sup>91</sup> Jason Kincaid, *The Looming Facebook Privacy Fiasco* (July 1, 2009),

<http://www.techcrunch.com/2009/07/01/the-looming-facebook-privacy-fiasco/>.

<sup>92</sup> *Id.*

85. Following the changes in Facebook privacy settings, noted blogger Danny Sullivan wrote, "I came close to killing my Facebook account this week." He went on to say, "I was disturbed to discover things I previously had as options were no longer in my control." Sullivan, the editor of Search Engine Land and an expert in search engine design,<sup>93</sup> concluded:

I don't have time for this. I don't have time to try and figure out the myriad of ways that Facebook may or may not want to use my information. That's why I almost shut down my entire account this week. It would be a hell of a lot easier than this mess.<sup>94</sup>

86. Carleton College librarian Iris Jastram states that the privacy trade-off resulting from the Facebook changes is not "worth it." She writes,

I'm already making concessions by making myself available to the students who want to friend me there and by grudgingly admitting that I like the rolodex function it plays. But I feel zero motivation to give up more than I can help to Facebook and its third party developers. They can kindly leave me alone, please.<sup>95</sup>

87. Chris Bourg, manager of the Information Center at Stanford University Libraries, notes that "[t]here are some concerns with the new default/recommended privacy settings, which make your updates visible to Everyone, including search engines."<sup>96</sup>

88. Reuters columnist Felix Salmon learned of Facebook's revised privacy settings when Facebook disclosed his "friends" list to critics, who republished the personal information. Salmon apologized to his friends and denounced the Facebook "Everyone" setting:

I'm a semi-public figure, and although I might not be happy with this kind of cyberstalking, I know I've put myself out there and that there will be consequences of that. But that decision of mine shouldn't have some kind

<sup>93</sup> Wikipedia, *Danny Sullivan (technologist)*, [http://en.wikipedia.org/wiki/Danny\\_Sullivan\\_\(technologist\)](http://en.wikipedia.org/wiki/Danny_Sullivan_(technologist)) (last visited Dec. 15, 2009).

<sup>94</sup> Danny Sullivan, *Now Is It Facebook's Microsoft Moment?* (Dec. 11, 2009), <http://dabble.com/facebook-microsoft-moment-1556>.

<sup>95</sup> Iris Jastram, *Dear Facebook: Leave Me Alone*, Pegasus Librarian Blog (Dec. 10, 2009), <http://pegasuslibrarian.com/2009/12/dear-facebook-leave-me-alone.html>.

<sup>96</sup> Chris Bourg, *Overview of new Facebook Privacy Settings*, Feral Librarian (Dec. 9, 2009), <http://chrisbourg.wordpress.com/2009/12/09/overview-of-new-facebook-privacy-settings/>.

of transitive property which feeds through to my personal friends, and I don't want the list of their names to be publicly available to everyone.<sup>97</sup>

89. In a blog post responding to the revisions, Marshall Kirkpatrick of ReadWriteWeb wrote, "the company says the move is all about helping users protect their privacy and connect with other people, but the new default option is to change from 'old settings' to becoming visible to 'everyone.' . . . This is not what Facebook users signed up for. It's not about privacy at all, it's about increasing traffic and the visibility of activity on the site."<sup>98</sup>

90. Jared Newman of PC World details Facebook's privacy revisions.<sup>99</sup> He is particularly critical of the "Everyone" setting:

By default, Facebook suggests sharing everything on your profile to make it 'easier for friends to find, identify and learn about you.' It should read, 'make it easier for anyone in the world to find, identify and learn about you.' A little creepier, sure, but this is part of Facebook's never-ending struggle to be, essentially, more like Twitter. Thing is, a lot of people like Facebook because it isn't like Twitter. Don't mess with a good thing.<sup>100</sup>

91. Rob Pegoraro blogged on the Washington Post's "Faster Forward" that the Facebook changes were "more of a mess than I'd expected." He criticized the revised "Everyone" privacy setting, stating the change "should never have happened. *Both from a usability and a PR perspective, the correct move would have been to leave users' settings as they were, especially for those who had already switched their options from the older defaults.*"<sup>101</sup>

92. In another Washington Post story, Cecilia Kang warned users, "post with care."<sup>102</sup> According to Kang:

While Facebook users will be able to choose their privacy settings, the problem is that most people don't take the time to do so and may simply

<sup>97</sup> Felix Salmon, *Why Can't I Hide My List of Facebook Friends?*, Reuters (Dec. 10, 2009), <http://blogs.reuters.com/felix-salmon/2009/12/10/why-cant-i-hide-my-list-of-facebook-friends/>.

<sup>98</sup> Marshall Kirkpatrick, ReadWriteWeb, *The Day Has Come: Facebook Pushes People to Go Public*, [http://www.readriteweb.com/archives/facebook\\_pushes\\_people\\_to\\_go\\_public.php](http://www.readriteweb.com/archives/facebook_pushes_people_to_go_public.php) (last visited Dec. 14, 2009).

<sup>99</sup> [http://www.pcworld.com/article/184465/facebook\\_privacy\\_changes\\_the\\_good\\_and\\_the\\_bad.html](http://www.pcworld.com/article/184465/facebook_privacy_changes_the_good_and_the_bad.html)

<sup>100</sup> *Id.*

<sup>101</sup> Rob Pegoraro, *Facebook's new default: Sharing updates with 'Everyone'*, Washington Post, Dec. 10, 2009, available at [http://voices.washingtonpost.com/fasterforward/2009/12/facebook\\_default\\_no-privacy.html](http://voices.washingtonpost.com/fasterforward/2009/12/facebook_default_no-privacy.html) (emphasis added)

<sup>102</sup> Cecilia Kang, *Facebook adopts new privacy settings to give users more control over content*, Washington Post, Dec. 10, 2009, available at <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/09/AR2009120904200.html?hpid=topnews>.

stick with the defaults. Others may find the process confusing and may not understand how to adjust those settings. Facebook said about one in five users currently adjusts privacy settings.<sup>103</sup>

93. New York Times technology writer Brad Stone reported that these changes have not been welcomed by many users.<sup>104</sup> One user wrote:

It's certainly a violation of my privacy policy. My own 'personal' privacy policy specifically states that I will not share information about my friends with any potential weirdos, child molesters, homicidal maniacs, or anyone I generally don't like.<sup>105</sup>

94. Stone invited readers to comment on their understanding of the changes. Of the more than 50 responses received, most expressed confusion, concern, or anger. One user explained,

I find the changes to be the exact opposite of what Facebook claims them to be. Things that were once private for me, and for carefully selected Facebook friends, are now open to everyone on the Internet. This is simply not what I signed up for. These are not the privacy settings I agreed to. It is a complete violation of privacy, not the other way around.<sup>106</sup>

95. Another Facebook user wrote,

There are users like myself that joined Facebook because we were able to connect with friends and family while maintaining our privacy and now FB has taken that away. Im [*sic*] wondering where are the millions of users that told FB it would be a good idea to offer real-time search results of their FB content on Google.<sup>107</sup>

96. A Boston Globe editorial, "Facebook's privacy downgrade," observes that "Facebook's subtle nudges toward greater disclosure coincided with other disconcerting changes: The site is treating more information, such as a user's home city and photo, as 'publicly available information' that the user cannot control. Over time, privacy changes can only

<sup>103</sup> *Id.*

<sup>104</sup> Brad Stone, *Facebook's Privacy Changes Draw More Scrutiny*, N.Y. Times, Dec. 10, 2009, available at <http://bits.blogs.nytimes.com/2009/12/10/facebook-privacy-changes-draw-more-scrutiny>.

<sup>105</sup> *Id.*

<sup>106</sup> *Id.*

<sup>107</sup> Riva Richmond, *The New Facebook Privacy Settings: A How-To*, N.Y. Times, Dec. 11, 2009, available at <http://gadgetwise.blogs.nytimes.com/2009/12/11/the-new-facebook-privacy-settings-a-how-to/?em>.

alienate users.” Instead, the Globe argues, “Facebook should be helping its 350 million members keep more of their information private.”<sup>108</sup>

97. An editorial from the L.A. Times states simply “what’s good for the social networking site isn’t necessarily what’s good for users.”<sup>109</sup>

#### V. Legal Analysis

##### **The FTC’s Section 5 Authority**

98. Facebook is engaging in unfair and deceptive acts and practices.<sup>110</sup> Such practices are prohibited by the FTC Act, and the Commission is empowered to enforce the Act’s prohibitions.<sup>111</sup> These powers are described in FTC Policy Statements on Deception<sup>112</sup> and Unfairness.<sup>113</sup>
99. A trade practice is unfair if it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”<sup>114</sup>
100. The injury must be “substantial.”<sup>115</sup> Typically, this involves monetary harm, but may also include “unwarranted health and safety risks.”<sup>116</sup> Emotional harm and other “more subjective types of harm” generally do not make a practice unfair.<sup>117</sup> Secondly, the injury “must not be outweighed by an offsetting consumer or competitive benefit that the

<sup>108</sup> Editorial, *Facebook’s privacy downgrade*, Boston Globe, Dec. 16, 2009, available at [http://www.boston.com/bostonglobe/editorial\\_opinion/editorials/articles/2009/12/16/facebooks\\_privacy\\_downgrade](http://www.boston.com/bostonglobe/editorial_opinion/editorials/articles/2009/12/16/facebooks_privacy_downgrade).

<sup>109</sup> Editorial, *The business of Facebook*, L.A. Times, Dec. 12, 2009, available at <http://www.latimes.com/news/opinion/editorials/la-ed-facebook12-2009dec12,0,4419776.story>.

<sup>110</sup> See 15 U.S.C. § 45.

<sup>111</sup> *Id.*

<sup>112</sup> Fed. Trade Comm’n, FTC Policy Statement on Deception (1983), available at <http://www.ftc.gov/bcp/policystmt/ad-decept.htm> [hereinafter FTC Deception Policy].

<sup>113</sup> Fed. Trade Comm’n, FTC Policy Statement on Unfairness (1980), available at <http://www.ftc.gov/bcp/policystmt/ad-unfair.htm> [hereinafter FTC Unfairness Policy].

<sup>114</sup> 15 U.S.C. § 45(n); see, e.g., *Fed. Trade Comm’n v. Seismic Entertainment Productions, Inc.*, Civ. No. 1:04-CV-00377 (Nov. 21, 2006) (finding that unauthorized changes to users’ computers that affected the functionality of the computers as a result of Seismic’s anti-spyware software constituted a “substantial injury without countervailing benefits.”).

<sup>115</sup> FTC Unfairness Policy, *supra* note 113.

<sup>116</sup> *Id.*; see, e.g., *Fed. Trade Comm’n v. Information Search, Inc.*, Civ. No. 1:06-cv-01099 (Mar. 9, 2007) (“The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers’ authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers.”).

<sup>117</sup> FTC Unfairness Policy, *supra* note 113.

sales practice also produces.”<sup>118</sup> Thus the FTC will not find a practice unfair “unless it is injurious in its net effects.”<sup>119</sup> Finally, “the injury must be one which consumers could not reasonably have avoided.”<sup>120</sup> This factor is an effort to ensure that consumer decision making still governs the market by limiting the FTC to act in situations where seller behavior “unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking.”<sup>121</sup> Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence highly susceptible classes of consumers.<sup>122</sup>

101. The FTC will also look at “whether the conduct violates public policy as it has been established by statute, common law, industry practice, or otherwise.”<sup>123</sup> Public policy is used to “test the validity and strength of the evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present.”<sup>124</sup>
102. The FTC will make a finding of deception if there has been a “representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer’s detriment.”<sup>125</sup>
103. First, there must be a representation, omission, or practice that is likely to mislead the consumer.<sup>126</sup> The relevant inquiry for this factor is not whether the act or practice actually misled the consumer, but rather whether it is likely to mislead.<sup>127</sup> Second, the act or practice must be considered from the perspective of a reasonable consumer.<sup>128</sup> “The test is whether the consumer’s interpretation or reaction is reasonable.”<sup>129</sup> The FTC will look at the totality of the act or practice and ask questions such as “how clear is the representation? How conspicuous is any qualifying information? How important is the

---

<sup>118</sup> *Id.*

<sup>119</sup> *Id.*

<sup>120</sup> *Id.*

<sup>121</sup> *Id.*

<sup>122</sup> *Id.*

<sup>123</sup> *Id.*

<sup>124</sup> *Id.*

<sup>125</sup> FTC Deception Policy, *supra* note 112.

<sup>126</sup> FTC Deception Policy, *supra* note 112; *see, e.g., Fed Trade Comm’n v. Pantron I Corp.*, 33 F.3d 1088 (9th Cir. 1994) (holding that Pantron’s representation to consumers that a product was effective at reducing hair loss was materially misleading, because according to studies, the success of the product could only be attributed to a placebo effect, rather than on scientific grounds).

<sup>127</sup> FTC Deception Policy, *supra* note 112.

<sup>128</sup> *Id.*

<sup>129</sup> *Id.*

omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?”<sup>130</sup>

104. Finally, the representation, omission, or practice must be material.<sup>131</sup> Essentially, the information must be important to consumers. The relevant question is whether consumers would have chosen another product if the deception had not occurred.<sup>132</sup> Express claims will be presumed material.<sup>133</sup> Materiality is presumed for claims and omissions involving “health, safety, or other areas with which the reasonable consumer would be concerned.”<sup>134</sup> The harms of this social networking site’s practices are within the scope of the FTC’s authority to enforce Section 5 of the FTC Act and its purveyors should face FTC action for these violations.

**Material Changes to Privacy Practices and  
Misrepresentations of Privacy Policies  
Constitute Consumer Harm**

105. Facebook’s actions injure users throughout the United States by invading their privacy; allowing for disclosure and use of information in ways and for purposes other than those consented to or relied upon by such users; causing them to believe falsely that they have full control over the use of their information; and undermining the ability of users to avail themselves of the privacy protections promised by the company.
106. The FTC Act empowers and directs the FTC to investigate business practices, including data collection practices, that constitute consumer harm.<sup>135</sup> The Commission realizes the importance of transparency and clarity in privacy policies. “Without real transparency, consumers cannot make informed decisions about how to share their information.”<sup>136</sup>
107. The FTC recently found that Sears Holding Management Corporations business practices violated the privacy of its customers.<sup>137</sup> The consent order arose from the company’s use of software to collect and disclose users’ online activity to third parties,

<sup>130</sup> *Id.*

<sup>131</sup> *Id.*

<sup>132</sup> *Id.*

<sup>133</sup> *Id.*

<sup>134</sup> *Id.*

<sup>135</sup> 15 U.S.C. § 45.

<sup>136</sup> Remarks of David C. Vladeck, Director, FTC Bureau of Consumer Protection, New York University: “Promoting Consumer Privacy: Accountability and Transparency in the Modern World” (Oct. 2, 2009).

<sup>137</sup> In re Sears Holdings Mgmt. Corp., No. C-4264 (2009) (decision and order), *available at* <http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf>.

and a misleading privacy policy that did not “adequately [inform consumers as to] the full extent of the information the software tracked.”<sup>138</sup> The order requires that the company fully, clearly, and prominently disclose the “types of data the software will monitor, record, or transmit.”<sup>139</sup> Further, the company must disclose to consumers whether and how this information will be used by third parties.<sup>140</sup>

108. The Commission has also obtained a consent order against an online company for changing its privacy policy in an unfair and deceptive manner. In 2004, the FTC charged Gateway Learning Corporation with making a material change to its privacy policy, allowing the company to share users’ information with third parties, without first obtaining users’ consent.<sup>141</sup> This was the first enforcement action to “challenge deceptive and unfair practices in connection with a company’s material change to its privacy policy.”<sup>142</sup> Gateway Learning made representations on the site’s privacy policy, stating that consumer information would not be sold, rented or loaned to third parties.<sup>143</sup> In violation of these terms, the company began renting personal information provided by consumers, including gender, age and name, to third parties.<sup>144</sup> Gateway then revised its privacy policy to provide for the renting of consumer information “from time to time,” applying the policy retroactively.<sup>145</sup> The settlement bars Gateway Learning from, among other things, “misrepresent[ing] in any manner, expressly or by implication . . . the manner in which Respondent will collect, use, or disclose personal information.”<sup>146</sup>

109. Furthermore, the FTC has barred deceptive claims about privacy and security policies with respect to personally identifiable, or sensitive, information.<sup>147</sup> In 2008, the FTC issued an order prohibiting Life is Good, Inc. from “misrepresent[ing] in any manner, expressly or by implication, the extent to which respondents maintain and protect the privacy, confidentiality, or integrity of any personal information collected

<sup>138</sup> In re Sears Holdings Mgmt. Corp., No. C-4264 (2009) (complaint), available at <http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf> (last visited Sep. 25, 2009).

<sup>139</sup> In re Sears Holdings Mgmt. Corp., No. C-4264 (2009) (decision and order), available at <http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf>.

<sup>140</sup> *Id.*

<sup>141</sup> Press Release, FTC, Gateway Learning Settles FTC Privacy Charges (July 7, 2004), <http://www.ftc.gov/opa/2004/07/gateway.shtm>.

<sup>142</sup> *Id.*

<sup>143</sup> In re Gateway Learning Corp., No. C-4120 (2004) (complaint), available at <http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf>.

<sup>144</sup> *Id.*

<sup>145</sup> *Id.*

<sup>146</sup> In re Gateway Learning Corp., No. C-4120 (2004) (decision and order), available at <http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf>.

<sup>147</sup> In re Life is Good, No. C-4218 (2008) (decision and order), available at <http://www.ftc.gov/os/caselist/0723046/080418do.pdf>.



from or about consumers.”<sup>148</sup> The company had represented to its customers, “we are committed to maintaining our customers’ privacy,” when in fact, it did not have secure or adequate measures of protecting personal information.<sup>149</sup> The Commission further ordered the company to establish comprehensive privacy protection measures in relation to its customers’ sensitive information.<sup>150</sup>

**Facebook’s Revisions to the Privacy Settings  
Constitute an Unfair and Deceptive Trade Practice**

110. Facebook represented that users “may not want everyone in the world to have the information you share on Facebook,” and that users “have extensive and precise controls available to choose who sees what among their network and friends, as well as tools that give them the *choice* to make a limited set of information available to search engines and other outside entities.”<sup>151</sup>
111. Facebook’s changes to users’ privacy settings and associated policies in fact categorize as “publicly available information” users’ names, profile photos, lists of friends, pages they are fans of, gender, geographic regions, and networks to which they belong.<sup>152</sup> Those categories of user data are no longer subject to users’ privacy settings.
112. Facebook represented that its changes to its policy settings and associated policies regarding application developers permit users to “opt-out of Facebook Platform and Facebook Connect altogether through [their] privacy settings,”<sup>153</sup> and tells users, “you can control how you share information with those third-party applications and websites through your application settings”<sup>154</sup>
113. Facebook’s changes to users’ privacy settings and associated policies regarding application developers in fact eliminate the universal one-click option for opting out of Facebook Platform and Facebook Connect, and replaces it with a less comprehensive

---

<sup>148</sup> *Id.*

<sup>149</sup> *Id.*

<sup>150</sup> *Id.*

<sup>151</sup> Testimony of Chris Kelly, Chief Privacy Officer, Facebook, Before the U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection Subcommittee on Communications, Technology and the Internet (June 18, 2009), *available at* [http://energycommerce.house.gov/Press\\_111/20090618/testimony\\_kelly.pdf](http://energycommerce.house.gov/Press_111/20090618/testimony_kelly.pdf).

<sup>152</sup> Facebook, *Privacy Policy*, <http://www.facebook.com/policy.php> (last visited Dec. 13, 2009).

<sup>153</sup> *Id.*

<sup>154</sup> *Id.*

option that requires users to provide application developers with personal information that users could previously prevent application developers from accessing.<sup>155</sup>

114. Facebook's representations regarding its changes to users' privacy settings and associated policies are misleading and fail to provide users clear and necessary privacy protections.
115. Wide opposition by users, commentators, and advocates to the changes to Facebook's privacy settings and associated policies illustrate that the changes injure Facebook users and harm the public interest.
116. Absent injunctive relief by the Commission, Facebook is likely to continue its unfair and deceptive business practices and harm the public interest.
117. Absent injunctive relief by the Commission, the privacy safeguards for consumers engaging in online commerce and new social network services will be significantly diminished.

#### VI. Prayer for Investigation and Relief

118. EPIC requests that the Commission investigate Facebook, enjoin its unfair and deceptive business practices, and require Facebook to protect the privacy of Facebook users. Specifically, EPIC requests the Commission to:

Compel Facebook to restore its previous privacy settings allowing users to choose whether to publicly disclose personal information, including name, current city, and friends;

Compel Facebook to restore its previous privacy setting allowing users to fully opt out of revealing information to third-party developers;

Compel Facebook to make its data collection practices clearer and more comprehensible and to give Facebook users meaningful control over personal information provided by Facebook to advertisers and developers; and

Provide such other relief as the Commission finds necessary and appropriate.

---

<sup>155</sup> Facebook, *Privacy Settings*, [http://www.facebook.com/settings/?tab=privacy&section=applications&field=friends\\_share](http://www.facebook.com/settings/?tab=privacy&section=applications&field=friends_share) (last visited Dec. 13, 2009).

119. EPIC reserves the right to supplement this petition as other information relevant to this proceeding becomes available.

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director  
John Verdi, EPIC Senior Counsel  
Kimberly Nguyen, EPIC Consumer Privacy Counsel  
Jared Kaprove, EPIC Domestic Surveillance Counsel  
Matthew Phillips, EPIC Appellate Advocacy Counsel  
Ginger McCall, EPIC National Security Counsel

ELECTRONIC PRIVACY INFORMATION CENTER  
1718 Connecticut Ave., NW Suite 200  
Washington, DC 20009  
202-483-1140 (tel)  
202-483-1248 (fax)

American Library Association  
The Center for Digital Democracy  
Consumer Federation of America  
FoolProof Financial Education  
Patient Privacy Rights  
Privacy Activism  
Privacy Rights Now Coalition  
The Privacy Rights Clearinghouse  
The U. S. Bill of Rights Foundation

December 17, 2009



April 10, 2018

Dear Chairman Walden and Ranking Member Pallone:

Although many are understandably focusing on the privacy implications of the Facebook-Cambridge Analytica incident, I encourage you to also consider this event in a broader context: how online platforms are increasingly at the center of scandals that raise serious social, economic, consumer protection, and safety issues, and how those scandals are beginning to overshadow these online platforms' benefits and erode public trust.

The internet has unquestionably revolutionized communication, commerce, and creativity. Yet there is a growing chorus of concern around a wave of problems resulting from a lack of online accountability.

In every other sector of our economy, the public rightfully expects companies to behave responsibly and to undertake reasonable efforts to prevent foreseeable harms associated with their products and services. When businesses fail to meet those obligations, they are ordinarily held accountable. For two decades, the internet has lived under a different set of rules and expectations, stemming largely from immunities and safe harbors put in place when the internet was in its infancy and looked nothing like it does today.

The internet is no longer nascent—and people around the world are growing increasingly uncomfortable with what it is becoming. As highlighted by the recent congressional debate around human trafficking, it is worth examining how we got to the point where some believe the rules simply don't apply and that platform immunity, whatever the cost, is the price the public must pay for a vibrant internet.

There was a vision for the internet, and this is not it. The moment has come for a national dialogue about restoring accountability on the internet. Whether through regulation, recalibration of safe harbors, or the exercise of greater responsibility by online platforms, something must change. I thank you for your leadership and look forward to working with you and your colleagues in the months ahead.

  
Charles H. Rivkin  
Chairman & CEO  
Motion Picture Association of America

cc: Members of the House Energy and Commerce Committee



The Honorable Greg Walden  
Chairman  
Committee on Energy and Commerce  
U.S. House of Representatives  
Washington, District of Columbia 20515

The Honorable Frank Pallone  
Ranking Member  
Committee on Energy and Commerce  
U.S. House of Representatives  
Washington, District of Columbia 20515

April 10, 2018

Dear Chairman Walden and Ranking Member Pallone:

ACT | The App Association appreciates the opportunity to comment on this important hearing to examine how companies use consumer data and communicate with consumers about those uses. This hearing, "Facebook: Transparency and Use of Consumer Data," affords us the opportunity to examine how the small companies that plug into larger platforms like Facebook handle these major issues. The sobering revelations around Cambridge Analytica have underscored that now more than ever, quietly seeking extraordinary data privacy permissions is not a viable approach. In this letter, we will share what we have learned through our efforts to educate on privacy law compliance and the development of best practices and describe the benefits of allowing some flexibility for consumers and companies to define permissible uses of data from the perspective of small tech businesses.

The app ecosystem is now valued at roughly \$143 billion and represents the front end for \$8 trillion in international trade annually. The impressive numbers produced by this powerful engine are driven by small enterprises. Most of our members range from one-person shops to a few hundred people at the most. Yet some of the most significant advances in data-driven industries, from healthcare and public safety to manufacturing and smart cities, come from small businesses like App Association member companies. This gives us a unique voice on data privacy issues.

The United States leads the world in digital innovation. Why? Because American companies are at the forefront of using data to produce beneficial services. With over seven million tech sector jobs, and a growth rate of 3 percent, the policy environment in the United States has produced a successful, data-driven economy, and countries all over the world are working to expand their tech sectors as well. We must take steps to ensure continued growth for the United States, while addressing the serious privacy problems this hearing sets out to explore.

With this statement, we hope members of the Committee take away the following:

- Our experience suggests that effective privacy protection requires a persistent dialogue between data collectors and consumers tailored to the circumstances of and purposes for data collection and use;

1401 K Street NW Suite 501  
Washington, DC 20005

📞 202.331.2130

🐦 @ACTonline

🌐 ACTonline.org

🌐 /actonline.org

- Industry groups like ACT | The App Association are working hard to ensure small and mid-sized firms understand how to comply with legal obligations, while leveraging competition in the market to create new approaches to protect privacy; and
- Overly intrusive government regulation of privacy—including strict data minimization or constant opt-in requirements—is suboptimal because it would interrupt the privacy dialogue that should be occurring between companies and consumers and may strip away uses of large data sets that are unforeseeable at the time of collection.

#### I. Industry Efforts to Enhance Consumer Privacy

Consumer privacy is a difficult concept to standardize because it can mean so many different things to different people. Further complicating the differing values and definitions of ideal privacy are the increasingly important and complex uses of data that pertain to individuals. The events that led to this hearing—a situation where consumer data was shared in a manner that appears consistent with an agreement's terms, but further uses by a third party were not authorized—illustrate these difficulties well. Nonetheless, the App Association has participated in and led several industry efforts to enhance consumers' options, develop best practices, and hold companies accountable for their actions related to consumer privacy. Some lessons learned in these processes may help the Committee as it considers possible market failure and its own role in better protecting consumer privacy.

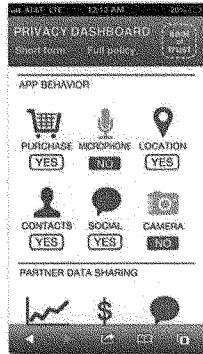
Most relevant to this hearing, the App Association a) executed the practical application of the National Telecommunications and Information Administration (NTIA) multistakeholder group's short form privacy notice; and b) led the creation of several compliance guides and best practices, including conducting privacy events called the mobile developer ("MoDev") series, the Health Insurance Portability and Accountability Act (HIPAA), and the European Commission's General Data Protection Directive (GDPR).

##### A. NTIA short form privacy notice

In 2013, NTIA hosted a multistakeholder working group gathering consumer groups together with industry to develop a voluntary code of conduct for mobile apps to clearly and concisely communicate how apps collect and use consumer data. The forum was convened pursuant to a White House "Privacy Blueprint," directing the U.S. Department of Commerce to gather stakeholders to build consensus around various aspects of consumer privacy.<sup>1</sup>

The final product called for signatories to the code of conduct to disclose any information they collect in eight key areas including biometrics and financial information, as well as whether they share with certain types of entities including ad networks and carriers. Stakeholders from the American Civil Liberties Union (ACLU) to Verizon supported the final code of conduct and on July 25, 2013, the group moved on to the testing phase. The App Association developed user interfaces and reported on consumer testing of some physical representations of the short form notice code of conduct. Some observations may be relevant as the Committee examines the issues raised by Cambridge Analytica's alleged retention and use of consumer data.

<sup>1</sup> <https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency>



First, in an effort to shorten privacy notices, the resulting privacy dashboard describing the basics of how and with whom an app shares data would leave out the “why.” During testing, consumers indicated that they were confused as to why a given app would collect certain information. For example, one consumer wondered why a fitness tracking app would collect financial information (perhaps the app would collect financial information only if the consumer purchased something through the app). Another wondered why an app shared any information with a social network and what that social network would do with the information. When consumers are asked to examine privacy policies closely and think about what app companies are doing with their data, questions quickly arise, and short form notice does not lend itself easily to an explanation of “why” certain data is collected or shared with certain entities.

Second, consumers were confused by notices using icons without interactive features. In the image above, types of data the app does not collect are signified with a faded icon and the word “NO.” But consumers looking to learn more about the app company’s decision-making with respect to their data were frustrated when tapping the icons did not pull up further details. This result suggests that a short and simple privacy notice should also include an option to learn more, as well as an option to turn on or off the app’s collection of a certain type of information, as some mobile platforms allow us to do now.

Third, participants in the testing did not understand the role of certain types of entities indicated in the short form notice. The types of companies they understood the least included “consumer data resellers” and “data analytics providers.” Thus, even when an app developer makes it clear that it shares specific types of data with data analytics providers, consumers lacked an understanding of what data analytics providers or consumer data resellers *do* with their information and the repercussions that could ensue.

The findings from our short form notice testing show that to be truly useful and accessible, privacy must be an interactive dialogue between the service and the consumer. As software has improved, we have better capabilities to facilitate this interaction and many of those improved functionalities have manifested themselves in the market. Even as small to mid-sized app developers like our member companies create innovative privacy dialogues with their users, the privacy options available on some platforms play an important role. The technical controls available for consumers—whether provided through the app or at the platform level—obviate

the need for platforms to conduct audits on apps to find out whether they are complying with a contractual term. That control is already vested in the consumer.

We have found that privacy controls on the iOS platform are highly effective and maintain the ability for app developers and consumers to share valuable information, which helps ensure their services remain free and the next great product is based on actionable data. Platform privacy options have the powerful attribute of not allowing app developers to circumvent them, which in turn gives app developers confidence that consumer wishes are being honored through the platform. However, the Committee should avoid governmental mandates that require such controls. Just as compliance with the bare minimum aspects of a voluntary program results in suboptimal privacy protections, so would a mandate remove the incentives for companies to compete and experiment with other solutions. Similarly, a mandate requiring a platform to conduct audits on all the apps that plug into it would have the perverse effect of pushing competitively sensitive information to the platform that could be used to advantage it against smaller potential competitors. Moreover, these mandates would incent companies to undertake those baseline measures to comply with the letter of the law, leading to stagnant privacy models that fail to grow with better technologies and evolving consumer needs.

#### B. Compliance Guides and Best Practices

Platforms can provide valuable privacy-enhancing functions for app developers and consumers. But App Association members do not rely completely on platforms to comply with global privacy laws on their behalf. The Cambridge Analytica situation underscores that platforms and the companies that use platforms to reach consumers are separate entities, and neither one can be completely responsible for the other. Small businesses like App Association members may not have the considerable resources of platform companies to hire compliance staff or attorneys, but they are often just as liable under privacy laws here and abroad. The App Association acts as a resource for small businesses by producing compliance guides that make legal privacy obligations understandable and accessible for small, growing companies.

In our GDPR compliance guide, we note that when app companies share data with a third-party data processor, they must always seek written assurance from the data processor of "sufficient guarantees" that it also complies with GDPR.<sup>2</sup> We counsel our member companies to play the game of "Mother, May I," with a controller's data (in many cases the platform company). The definitions and interrelationships contemplated in GDPR are complex, and explaining them in short form is extremely difficult. But the guide is an example of private sector efforts to ensure that even the smallest companies in the app ecosystem are observing the most stringent privacy laws on the books. We are making serious efforts to ensure that small and mid-sized firms in the app economy are not taking advantage of their distance from the consumer.

We note that GDPR is not necessary to keep companies honest in this regard and would not have stopped activities in which Cambridge Analytica is alleged to have engaged. If good actors like our member companies do not have the direct consumer relationship, they do not benefit from taking advantage of the opacity of their activities involving consumer data. Not only do those activities risk running afoul of U.S. privacy law, but they also undermine the trust on which those companies' brands are built. We have found that compliance with GDPR is extremely expensive and diverts resources away from needed areas of growth, and even privacy policy development. One App Association member company with just under 60 employees has dedicated 10 full-time staff to developing its own compliance program with GDPR. And once the

<sup>2</sup> [http://actonline.org/wp-content/uploads/ACT\\_GDPR-Guide\\_interactive.pdf](http://actonline.org/wp-content/uploads/ACT_GDPR-Guide_interactive.pdf)



program is completed, two full-time staff are likely to be tasked with continued compliance with the law. We want to be clear that while we seek to clarify our member companies' legal obligations under European privacy law, we have seen firsthand that the law imposes unnecessarily high costs on small businesses.

The advent of app platforms democratized app development, creating a pathway for mobile software entrepreneurs to reach consumers in a safe and secure environment. As soon as this increased access for small business took place, the App Association began its privacy outreach to developers through its MoDev series. Thus, we sought to democratize privacy best practices in equal measure to the spread of business opportunity to small businesses. We conducted these seminars throughout the country and reached thousands of developers, delivering the message that app developers are responsible for clearly describing which data they collect, why they collect it, and what they do with it. Ten years ago, many developers were aware that they performed analytics, but had a less firm grasp on the fact that these analytics required the collection and stewardship of sensitive personal data. We conveyed the message that not only does this collection impose a serious responsibility on developers, but that responsibility also may be defined by policymakers in Washington if they failed to take appropriate measures to account for privacy.

App Association member companies that develop connected devices or apps that deal with health information ("protected health information" or PHI in healthcare parlance) face a potentially steep compliance burden under HIPAA. Our "HIPAA Check" tool guides app developers through a series of questions to determine how they can comply with the rules.<sup>3</sup> Although the tool is not legal advice, it helps give app developers a sense of the steps they need to take in order to put themselves on the right track. At the end of the process, we give the app company an option to receive a full, detailed report based on its answers to the questions.

With these guides and tools, the App Association and similar industry groups are "democratizing" an understanding of privacy obligations to smaller companies that plug into larger platforms. The alleged activities of Cambridge Analytica are an outlier among companies that draw consumer data from platforms. Although these kinds of events can evoke in the general public a sense that tech companies have come unmoored from privacy principles and accountability for the sake of monetizing the consumer's data, reality is less alarming and not nearly as sensational. Big data-driven products and services are not the "wild west" when it comes to seeking permission and adhering to promises around authorized uses of data. Legal privacy obligations are real, they apply to even the smallest businesses, and we are happy to make those obligations clear and accessible.

## **II. Beneficial Uses of Data are Incompatible with Strict "Minimization" or "Opt-In" Requirements**

As the Committee considers its role in shaping future privacy obligations, we caution against inevitable calls to adopt a regulatory regime like Europe's, which could preclude some of the most innovative and life-saving corners of our economy. A mandate to delete information that has survived the purposes for which it was initially collected would clearly render Cambridge Analytica's alleged actions illegal, not just in violation of relevant contractual terms. But the mandate would also flush reams of data from the ecosystem that are being put to work to improve safety and create jobs.

<sup>3</sup> <https://app.actonline.org/hipaa/disclaimer>

Under GDPR, personal data may only be “collected for specified, explicit . . . purposes and not further processed in a manner that is incompatible with those purposes . . .”<sup>4</sup> The inherent nature of artificial intelligence makes this provision at least very difficult to comply with and in some cases impossible. The European rules also require companies to collect express “opt-in” consent before processing personal information, which must be “specific,” “unambiguous,” and made by “a statement or by a clear affirmative action.”<sup>5</sup> There are a number of reasons policymakers should weigh the beneficial applications of artificial intelligence against policies that would wipe them out along with harmful actions like those at issue in this hearing.

#### A. Healthcare

Data-driven healthcare services provide an important example of why regulatory approaches should allow for flexible uses of data. Flexible data privacy laws support American jobs and can also save lives. The future of medicine is in data and artificial (or “augmented”) intelligence, tools that enhance the diagnostic and treatment capabilities of healthcare providers. A successful physician might see about 15,000 patients throughout her career, but recent innovations in technology have grown providers’ reach and effectiveness exponentially. Our members create data-driven platforms that enable doctors to make decisions based on hundreds of thousands, even millions, of examples. For instance, with these clinical decision support tools, a doctor can plug in a patient’s characteristics and see which medication is most likely to work. But this functionality only works if the characteristics can be matched against countless data points that a strict data minimization mandate would require to have been deleted.

Cancer clusters provide another important example. Researchers have long puzzled over why certain types of cancer occur in certain regions at higher rates than other parts of the country. In order to truly examine the various sets of circumstances and factors that may play a role in these higher rates, sensitive data must be collected and processed in ways that are not initially foreseeable. A series of data points that may seem to have nothing to do with cancer could become the key to combating it, and requiring them to be deleted pulls the rug out from our cancer curing efforts.

These advantages benefit everyone, and yes, they can save lives. But they can only exist when personal data can be collected for purposes beyond those that can be articulated with specificity at the outset and stored despite having served their initial purposes. Moreover, a mandate that requires constantly seeking unambiguous, precise consent from consumers serves as an interruption of an ongoing privacy dialogue that should be taking place between a consumer and app developer. Our member companies know that policies requiring the deletion of personal information that does not have a perfectly defined purpose at the time it is collected seriously degrade these life-saving capabilities.

#### B. Self-Driving Vehicles

Machine learning, a subset of artificial intelligence, animates the other engines in self-driving cars—the autonomous driving application. Just as the physical engines run on energy, the

<sup>4</sup> <https://gdpr-info.eu/art-5-gdpr/>

<sup>5</sup> <https://gdpr-info.eu/art-6-gdpr/>; <https://gdpr-info.eu/art-4-gdpr/>

autonomous driving engine runs on data from drivers and traffic patterns from around the globe. How can a self-driving car recognize a the trajectory of another car or an animal crossing the road? How does it know the animal is not a tree or a bush? The machine-learning engine that cars use must have seen animals in all their forms, in millions of different contexts. American car companies must collect data that is inevitably personal in nature in order to inform the software that drives these cars. The data must be held and processed for an indefinite period of time and for a set of purposes that are not explicit, except insofar as they serve as a representation or example for the software to compare against countless other examples.

As self-driving cars evolve and their machine-learning engines improve, the data that serves as the basis for the machine-learning engine may be used in ways that are not foreseeable now and yet produce substantial safety benefits. Unlike livestock or pets that might cross a road, which to the software are “known unknowns,” these are the “unknown unknowns”—potential threats that are not well enough understood to articulate them at the time images or other impressions of them are collected. If Congress were to enact policies requiring car companies to delete personal data (pictures of pedestrians for example) as soon as its future purposes are “incompatible” with the initial purpose, it would encumber their ability not just to create jobs, but also to save lives.

#### C. Business Intelligence

You may not realize that, on average, it takes your local coffee shop longer to make cold drinks than hot drinks. But the nation’s coffee chains are acutely aware, and longer processes require more workers behind the counter. Coffee chains have discovered that warmer weather leads to more cold drink purchases, at different rates depending on which part of the country you are located. In one city, coffee consumers may switch at much higher rates to cold drinks for every five-degree rise in temperature than in another city. Other types of weather features likely play a role as well. Coffee chains use these trends to predict staffing levels as many days in advance as possible, to handle the longer time it takes to make cold drinks. All of this analysis requires the collection and processing of data indicating human behavior, which could include personal information. But coffee chains and other types of consumer-facing businesses do not only care about how weather affects consumer behavior—countless other factors play a role in necessary staffing levels and supply needs. We simply cannot predict which factors will tend to create which outcomes and strict data minimization and explicit opt-in consent models require this kind of prediction or else the data must not exist.

### III. Conclusion

The revelations that brought about this Committee’s examination of consumer data privacy are alarming examples of how data revealing patterns in human behavior can be used against consumer expectations. It is often said that consumer privacy is about context—but more than that, it is about time and location. We appreciate the opportunity to share the lessons we have learned from our experiences in providing compliance assistance but also in creating the user interface for best practices. We urge the Committee to take a cautious approach when considering policies that would negate the beneficial uses of data to try and obviate abuses. An approach that errs on the side of hamstringing data usage not only prevents the unforeseeable, yet beneficial, uses of that data, but it also subverts the approach to privacy that respects the ongoing and just-in-time dialogue companies that use data should be having with their customers.

Sincerely,



Morgan Reed  
President  
ACT | The App Association



**Committee For Justice**  
Holding Judges and Politicians Accountable to the Constitution

The Committee for Justice  
1629 K St. NW Suite 300  
Washington, D.C. 20006

(202) 270-7748  
committeeofjustice.org  
CmteForJustice

April 10, 2018

The Honorable Greg Waldren  
Chairman, Committee on Energy and Commerce  
2185 Rayburn House Office Building  
Washington, D.C. 20515

The Honorable Frank Pallone  
Ranking Member, Committee on Energy and Commerce  
237 Cannon House Office Building  
Washington, D.C. 20515

---

**RE: Facebook: Transparency and Use of Consumer Data**

Dear Chairman Walden and Ranking Member Pallone,

We write to you regarding your April 11 hearing, "Facebook: Transparency and Use of Consumer Data." We, the president and public policy director of the Committee for Justice (CFJ), are concerned that the hearing will lead to the introduction of new legislation regulating online data collection and use. We are convinced such legislation is not only unnecessary but, if enacted, would also hurt consumers, threaten the online ecosystem that has transformed our daily lives, and negatively impact our country's economic growth.

Founded in 2002, CFJ is a nonprofit, nonpartisan legal and policy organization that educates the public and policymakers about and promotes the rule of law and constitutionally limited government. Consistent with this mission, CFJ engages in the national debate about a variety of tech policy issues, including advocating for digital privacy protections in Congress, the federal courts, and the news media.<sup>1</sup>

We have concluded that a legislative solution to the data privacy issues being discussed at the hearing would be detrimental to our nation for the following reasons:

- **Government-imposed restrictions on data collection would undercut economic growth, the vibrancy of the online ecosystem, and consumer satisfaction.** In recent decades, consumers' personal and professional lives have been transformed for the better by a vast collection of data-driven online resources that are made available to consumers for no cost because they are subsidized by advertising. These resources have also been an engine of economic growth, even during difficult economic times. For example, more than 70 million small businesses now use Facebook to grow and create jobs.<sup>2</sup> In particular, data-driven marketing, at issue in this hearing, is estimated to have added more than \$200 billion to the U.S. economy in 2014, a 35% increase over just two years earlier.<sup>3</sup> Government-imposed restrictions on such marketing would slow or reverse this economic growth, while hurting consumers by causing the demise of many of the data-driven online resources they rely on.

<sup>1</sup> See, e.g., amicus briefs filed in *Carpenter v. United States*. August 2017. <https://www.scribd.com/document/356288790/Amicus-Brief-Filed-in-Carpenter-v-United-States-and-United-States-v-Kolsuz>. March 2017. [https://www.scribd.com/document/355249553/United-States-v-Kolsuz-Amicus-Brief-Letter to Congress in support of the CLOUD Act](https://www.scribd.com/document/355249553/United-States-v-Kolsuz-Amicus-Brief-Letter-to-Congress-in-support-of-the-CLOUD-Act). March 2018. <https://www.committeeforjustice.org/single-post/support-clarifying-lawful-use-data>.

<sup>2</sup> *Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy & Commerce*, 115th Cong. (2018) (statement of Mark Zuckerberg).

<sup>3</sup> Deighton, John and Johnson, Peter. "The Value of Data 2015: Consequences for Insight, Innovation and Efficiency in the U.S. Economy." Data & Marketing Association. Dec. 2015. <http://thedma.org/advocacy/data-driven-marketing-institute/value-of-data>.

- **Legislation designed to reign in big companies like Facebook will inevitably harm small companies and tech startups the most.** When regulations restrict companies' ability to collect and use data, advertisers and other online companies experience decreased revenue. Large companies can typically survive these decreases in revenue, while small companies are often driven out of business. The vast majority of Internet companies fall in the latter category and include the very companies that might otherwise grow to compete with and even supplant Facebook and the other tech giants of today. The European Union's Privacy and Electronic Communications Directive (2002/58/EC) provides an unfortunate example of the harm privacy regulations can inflict on small businesses.<sup>4</sup> It is one reason why there are relatively few technology start-ups in Europe and most of them struggle to receive venture capital funding.<sup>5</sup>
- **The best way to provide consumers with data privacy solutions that meet their needs is competition in the Internet marketplace.** In contrast, increased government regulation of data privacy will stifle competition, in part because only larger companies can afford the increased compliance costs and reductions in revenue. This hearing will undoubtedly include questions about balancing the tradeoffs between privacy and the ability to share our lives, make our voices heard, and build online communities through social media. It makes little sense for Congress to impose a one-size-fits-all answer to these questions, given that individuals value the tradeoffs very differently. Addressing data privacy through competition, on the other hand, allows consumers to answer these questions for themselves according to their individual values.
- **Public opinion polls showing support for stronger data protections are misleading because they rarely confront consumers with the monetary of and other costs of their choices.**<sup>6</sup> A 2016 study found that, despite most participants' unease with an email provider using automated content analysis to provide more targeted advertisements, 65 percent of them were unwilling to pay providers *any* amount for a privacy-protecting alternative.<sup>7</sup> However, in the real world, consumers will lose free email and social media if government-imposed privacy regulations cut into providers' advertising revenue. Moreover, such studies remind us that most consumers do not value data privacy enough to pay anything for it. That should not be too surprising considering that today's thriving but largely unregulated social media ecosystem is not something that was thrust upon consumers or arose from factors beyond their control. Instead, it arose through the collective choices and values tradeoffs of billions of consumers.
- **New, punitive data privacy legislation is unnecessary because legal safeguards already exist.** In addition to industry self-regulation, consumers of social media and other Internet services are protected by the Federal Trade Commission's vigorous enforcement of its data privacy and security standards, using the prohibition against "unfair or deceptive" business

<sup>4</sup> OJ L 201, 31.7.2002, p. 37–47, ELI: <http://data.europa.eu/eli/dir/2002/58/oj>.

<sup>5</sup> Scott, Mark. "For Tech Start-Ups in Europe, an Oceanic Divide in Funding." *The New York Times*. January 19, 2018. <https://www.nytimes.com/2015/02/14/technology/for-tech-start-ups-in-europe-an-oceanic-divide-in-funding.html>.

<sup>6</sup> McQuinn, Alan. "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules." Information Technology and Innovation Foundation. Oct.6, 2017. <https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules>.

<sup>7</sup> Strahilevitz, Lior Jacob, and Matthew B. Kugler. "Is Privacy Policy Language Irrelevant to Consumers?" *The Journal of Legal Studies* 45, no. S2. Sept. 9, 2016. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2838449](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2838449).

practices in Section 5 of the Federal Trade Commission Act 15 U.S.C. §45(a).<sup>8</sup> In addition, state attorneys general enforce similar laws at the state level.<sup>9</sup>

- **The Cambridge Analytica incident that sparked this hearing must be put in perspective.** It is important to remember that the personal data disclosed by Facebook to an academic app builder named Aleksandr Kogan was not the sort of highly private data—credit card numbers, health records, and the like—that is sometimes stolen by hackers to the great detriment of consumers.<sup>10</sup> The data disclosed by Facebook came from the profiles of its users and consisted mostly of names, hometowns, and page likes—in other words, the type of data most people on Facebook are public about.<sup>11</sup> However, even that data is no longer available to app developers today. Kogan got the idea before Facebook tightened its data privacy policies in 2014.<sup>12</sup> Finally, the concern that has focused so much attention on the Kogan incident—claims that the data was used by Cambridge Analytica to put Donald Trump over the top in 2016—have little basis in fact. Cambridge used the Facebook data to run voter-targeted ads for political campaigns, but it appears that those ads were neither effective nor used in the Trump campaign.<sup>13</sup>
- **Because there is no crisis requiring urgent action and because no one yet fully understands the extent and nature of the privacy risks posed by Facebook's now discontinued policies, calls for government-imposed regulation are premature.** Replacing the light-touch regulation of data privacy currently provided by the FTC and state law with more heavy-handed federal legislation should be a last resort, not the reflexive response to news headlines. Consider also that the Cambridge Analytica incident would not be dominating the news but for the report, apparently incorrect, that the data in question was used to elect Donald Trump president.<sup>14</sup> Nor would the news coverage be so negative. Contrast that with the widely documented use of Facebook data in Barack Obama's 2012 presidential campaign, which was portrayed in a vastly different light by the news media and did not set off calls for Congressional

<sup>8</sup> See, e.g., Federal Trade Commission. *FTC Staff Report: Self-regulatory Principles for Online Behavioral Advertising*. 2009. <https://www.ftc.gov/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral>; Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace*. 2000. <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.

<sup>9</sup> Widman, Amy, and Prentiss Cox. "State Attorneys General Use of Concurrent Public Enforcement Authority in Federal Consumer Protection Laws." *SSRN Electronic Journal*, 2011. doi:10.2139/ssrn.1850744.

<sup>10</sup> Iraklis Symeonidis, Pagona Tsormpatzoudi, and Bart Preneel. *Collateral Damage of Online Social Network Applications*. 2016. <https://eprint.iacr.org/2015/456.pdf>; Ruffini, Patrick. "The Media's Double Standard on Privacy and Cambridge Analytica." Medium. March 20, 2018. <https://medium.com/@PatrickRuffini/the-medias-double-standard-on-privacy-and-cambridge-analytica-1e37ef0649da>.

<sup>11</sup> Albright, Jonathan. "The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle." Medium. March 20, 2018. <https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747>.

<sup>12</sup> Facebook. "The New Facebook Login and Graph API 2.0." Facebook for Developers. April 30, 2014. <https://developers.facebook.com/blog/post/2014/04/30/the-new-facebook-login>.

<sup>13</sup> Kavanagh, Chris. "Why (almost) Everything Reported about the Cambridge Analytica Facebook 'Hacking' Controversy Is Wrong." Medium. March 26, 2018. [https://medium.com/@CKava/why-almost-everything-reported-about-the-cambridge-analytica-facebook-hacking-controversy-is-d7f78af2d042?mc\\_cid=849ab4c39f&mc\\_eid=5a60ec2d43](https://medium.com/@CKava/why-almost-everything-reported-about-the-cambridge-analytica-facebook-hacking-controversy-is-d7f78af2d042?mc_cid=849ab4c39f&mc_eid=5a60ec2d43).

<sup>14</sup> See, e.g., Wood, Paul. "The British Data-crunchers Who Say They Helped Donald Trump to Win." *The Spectator*. December 01, 2016. <http://www.spectator.co.uk/2016/12/the-british-data-crunchers-who-say-they-helped-donald-trump-to-win/>; Taggart, Kendall. "The Truth About The Trump Data Team That People Are Freaking Out About." *BuzzFeed*. February 16, 2017. [https://www.buzzfeed.com/kendalltaggart/the-truth-about-the-trump-data-team-that-people-are-freaking-out?utm\\_term=.it3kDeoJYn#.myDn1Kd9rJ](https://www.buzzfeed.com/kendalltaggart/the-truth-about-the-trump-data-team-that-people-are-freaking-out?utm_term=.it3kDeoJYn#.myDn1Kd9rJ); Kroll, Andy. "Cloak and Data: The Real Story behind Cambridge Analytica's Rise and Fall." *Mother Jones*. March 26, 2018. <https://www.motherjones.com/politics/2018/03/cloak-and-data-cambridge-analytica-robert-mercer>.

hearings or new privacy legislation.<sup>15</sup> The important point is that allowing unhappiness with the 2016 election results to drive a push for increased government regulation and control of the Internet is a very bad way to make policy.

- **A rush to enact date privacy legislation is particularly dangerous in light of the glacial pace with which Congress will respond to the need for modernizing the legislation as technology rapidly evolves.** Consider the example of the Electronic Communications Privacy Act of 1986 (ECPA), which governs law enforcement's access to stored electronic data, such as emails. As storage of such data moved to the cloud, the ECPA became hopelessly obsolete, leading to increasingly concerned calls for its modernization from industry, law enforcement, and the White House. Despite those calls, it took many years for Congress to act by passing the Clarifying Lawful Overseas Use of Data or CLOUD Act in March of this year. And even then, Congress acted primarily because a Supreme Court case, *U.S. v. Microsoft*, forced them to.<sup>16</sup> There is good reason to believe that any legislation that comes out of this hearing will similarly remain in effect, unchanged, long after today's technological and privacy landscape has morphed into something we cannot fathom in 2018. In contrast, the self-regulation continuously being improved by Facebook and similar companies not only allows adaptation to technological change with far greater speed but also allows those companies to tailor data privacy solutions to the specific features of their platforms, rather than trying to conform with a one-size-fits-all federal mandate.

In sum, rushing to enact new legislation regulating online data collection and use would hinder innovation in the rapidly evolving world of social media and data-driven marketing, lessen consumer choice, and negatively impact our nation's economic growth.

We ask that this letter be entered in the hearing record. We thank you for your oversight of this important issue.

Sincerely,

Curt Levey  
*President*  
 The Committee for Justice

Ashley Baker  
*Director of Public Policy*  
 The Committee for Justice

<sup>15</sup> See Pilkington, Ed, and Amanda Michel. "Obama, Facebook and the Power of Friendship: The 2012 Data Election." *The Guardian*. February 17, 2012. <https://www.theguardian.com/world/2012/feb/17/obama-digital-data-machine-facebook-election>; Michael Scherer. "Friended: How the Obama Campaign Connected with Young Voters." *TIME*. November 20, 2012. <http://swampland.time.com/2012/11/20/friended-how-the-obama-campaign-connected-with-young-voters>.

<sup>16</sup> Levey, Curt. "Your email privacy will get a boost thanks to the omnibus spending bill (and that's a good thing)." *Fox News*. March 22, 2018. <http://www.foxnews.com/opinion/2018/03/22/your-email-privacy-will-get-boost-thanks-to-omnibus-spending-bill-and-thats-good-thing.html>.





**Mark Zuckerberg, CEO**  
 Facebook  
 1 Hacker Way,  
 Menlo Park, CA 94025.

Monday April 9, 2018

Dear Mr. Zuckerberg,

We write to you on behalf of leading consumer and privacy organizations, members of the Transatlantic Consumer Dialogue, in the United States and Europe to urge you to adopt the General Data Protection Regulation as a baseline standard for all Facebook services. There is simply no reason for your company to provide less than the best legal standards currently available to protect the privacy of Facebook users. We urge you to confirm your company's commitment to global compliance with the GDPR and provide specific details on how the company plans to implement these changes in your testimony before the US Congress this week.

The GDPR helps ensure that companies such as yours operate in an accountable and transparent manner, subject to the rule of law and the democratic process. The GDPR provides a solid foundation for data protection, establishing clear responsibilities for companies that collect personal data and clear rights for users whose data is gathered. These are protections that all users should be entitled to no matter where they are located.

We favor the continued growth of the digital economy and we strongly support innovation. The unregulated collection and use of personal data threatens this future. Data breaches, identity theft, cyber-attack, and financial fraud are all on the rise. The vast collection of personal data has also diminished competition. And the targeting of internet users, based on detailed and secret profiling with opaque algorithms, threatens not only consumer privacy but also democratic institutions.

We urge you to make clear your commitment to comply with the GDPR standards in all jurisdictions for all users, and we hope that your leadership on this issue will prompt others to make similar commitments.

Yours sincerely



**Jeffrey Chester**  
 Executive Director,  
 Center for Digital Democracy  
 U.S. Co-Chair, Digital Policy Committee



**Finn Lützow-Holm Myrstad**  
 Head of the Digital Services Section,  
 Norwegian Consumer Council (NCC)  
 EU Co-Chair, Digital Policy Committee

CC: Senate Leader Mitch McConnell and Senate Minority Leader Charles Schumer  
 House Speaker Paul Ryan and House Minority Leader Nancy Pelosi  
 FTC Acting Chair Maureen Olhausen and FTC Commissioner Terrel McSweeney  
 EU Council President Donald Tusk, EU Commissioner Věra Jourova, EP President Antonio Tajani,  
 EDPS Giovanni Buttarelli, Art29WP Chair Andrea Jelinek

October 30, 2017

Mr. Mark Zuckerberg, Chief Executive Officer  
Ms. Sheryl Sandberg, Chief Operating Officer  
Facebook, Inc.  
1 Hacker Way  
Menlo Park, CA 94025

Dear Mr. Zuckerberg and Ms. Sandberg,

We, the undersigned civil rights, interfaith, and advocacy organizations write to express our deep concern regarding ads, pages, and hateful content on your platform used to divide our country, and in particular, to promote anti-Muslim, anti-Black, anti-immigrant, and anti-LGBTQ animus. We thank you for recent meetings with some of our organizations representing communities that were directly affected by the material on your platform. We appreciate that senior members of your team—including you, Ms. Sandberg—have facilitated these meetings, and we hope that these conversations are the beginning of a serious and ongoing dialogue. Now, it is necessary for Facebook to take critical steps to address the bigotry and discrimination generated on your platform.

As you know, we do not yet have access to all the divisive content targeting communities we represent; therefore, we are only able to cite to the few examples that were leaked to the media.

For example, Russian operatives set up misleading accounts impersonating or posing as American individuals and groups on Facebook to promote Russian propaganda during the American election season. Reports indicate that a Russian Facebook account called “SecuredBorders” posed as a group of US citizens concerned about the increased number of refugees in America. This fake account not only promoted anti-immigrant messaging online, but also managed to organize an in-person anti-refugee rally in Twin Falls, Idaho in August 2016.<sup>1</sup>

In addition, a Facebook page entitled “United Muslims of America” was an imposter account traced back to Russia<sup>2</sup>—the real United Muslims of America is a California-based interfaith organization working at the local level to promote dialogue and political participation.<sup>3</sup> The imposter account smeared political candidates and

---

<sup>1</sup> Geoffrey Smith, “Russia Orchestrated Anti-Immigrant Rallies in the U.S. via Facebook Last Year,” *Fortune*, Sept. 12, 2017, *available at* <http://fortune.com/2017/09/12/russia-orchestrated-anti-immigrant-rallies-in-the-u-s-via-facebook-last-year/>.

<sup>2</sup> Dean Obeidallah, “How Russian Hackers Used My Face to Sabotage Our Politics and Elect Trump,” *The Daily Beast*, Sept. 27, 2017, *available at* <https://www.thedailybeast.com/how-russian-hackers-used-my-face-to-sabotage-our-politics-and-elect-trump>.

<sup>3</sup> United Muslims of America “About” page, *available at* <http://www.umanet.org/about-us>.

Facebook, Inc  
 October 30, 2017  
 Page 2 of 5

promoted political rallies aimed at Muslim audiences.<sup>4</sup> In another example, the Internet Research Agency in Russia promoted an anti-Muslim rally thousands of miles away in Houston, Texas where individuals protested outside of a mosque.<sup>5</sup> Additional reports indicate that Facebook offered its expertise to a bigoted advocacy group by creating a case study testing different video formats, and advising on how to enhance the reach of the group's anti-refugee campaign in swing states during the final weeks of the 2016 election.<sup>6</sup> These examples of content on Facebook were not only harmful, but also used to rile up supporters of President Trump.

Furthermore, it has been reported that Russian operatives purchased Facebook ads about Black Lives Matter—some impersonating the group and others describing it as a threat.<sup>7</sup> This included ads that were directly targeted to reach audiences in Ferguson, Missouri and Baltimore, Maryland. CNN reports that the Russian Internet Research Agency used these ads in an attempt to amplify political discord and create a general atmosphere of incivility and chaos.<sup>8</sup> This included a fake ad containing an image of an African-American woman dry-firing a rifle, playing on the worst stereotypes regarding African-Americans as threatening or violent.<sup>9</sup>

We were alarmed to see your platform being abused to promote bigotry, and especially disappointed that it has taken media exposure and congressional oversight to give a degree of transparency into your practices. It is important to keep in mind that pervasive bigotry has long existed on your platform, and the Russian operatives

---

<sup>4</sup> Obeillah, *supra* note 1.

<sup>5</sup> Tim Lister & Clare Sebastian, "Stoking Islamophobia and secession in Texas - from an office in Russia," CNN Politics, Oct. 6, 2017, *available at* <http://www.cnn.com/2017/10/05/politics/heart-of-texas-russia-event/index.html>.

<sup>6</sup> Melanie Ehrenkranz, "Facebook Reportedly Used Anti-Muslim Ad as Test Case in Video Formats," Gizmodo, Oct. 18, 2017, *available at* <https://gizmodo.com/facebook-reportedly-used-anti-muslim-ad-as-test-case-in-1819645900>.

<sup>7</sup> Adam Entous, Craig Timberg, & Elizabeth Dwoskin, "Russian operatives used Facebook ads to exploit America's racial and religious divisions," The Washington Post, Sept. 25, 2017, *available at* [https://www.washingtonpost.com/business/technology/russian-operatives-used-facebook-ads-to-exploit-divisions-over-black-political-activism-and-muslims/2017/09/25/4a011242-a21b-11e7-ade1-76d061d56efa\\_story.html?tid=sm\\_tw&utm\\_term=.e49cecc1a834](https://www.washingtonpost.com/business/technology/russian-operatives-used-facebook-ads-to-exploit-divisions-over-black-political-activism-and-muslims/2017/09/25/4a011242-a21b-11e7-ade1-76d061d56efa_story.html?tid=sm_tw&utm_term=.e49cecc1a834).

<sup>8</sup> Dylan Byers, "Exclusive: Russian-bought Black Lives Matter ad on Facebook targeted Baltimore and Ferguson," CNN Media, Sept. 28, 2017, *available at* <http://money.cnn.com/2017/09/27/media/facebook-black-lives-matter-targeting/index.html>.

<sup>9</sup> Adam Entous, Craig Timberg, & Elizabeth Dwoskin, "Russian Facebook ads showed a black woman firing a rifle, amid efforts to stoke racial strife," The Washington Post, Oct. 2, 2017, *available at* [https://www.washingtonpost.com/business/technology/russian-facebook-ads-showed-a-black-woman-firing-a-rifle-amid-efforts-to-stoke-racial-strife/2017/10/02/e4e78312-a785-11e7-b3aa-c0e2e1d41e38\\_story.html?utm\\_term=.aa2267a2f46c](https://www.washingtonpost.com/business/technology/russian-facebook-ads-showed-a-black-woman-firing-a-rifle-amid-efforts-to-stoke-racial-strife/2017/10/02/e4e78312-a785-11e7-b3aa-c0e2e1d41e38_story.html?utm_term=.aa2267a2f46c).

Facebook, Inc  
October 30, 2017  
Page 3 of 5

simply exploited the hateful content and activity already present. We are concerned about how a platform like Facebook's could operate without appropriate safeguards that take into account how it could be manipulated to further sow divisions in our society.

As a company and social network platform whose mission is "to give people the power to build community and bring the world closer together,"<sup>10</sup> we hope that you understand the gravity of this hateful rhetoric and behavior. During a time when anti-Muslim, anti-Black, anti-LGBTQ, and anti-immigrant sentiment has swept the nation, it is more important than ever for companies like yours to take an unequivocal stance against bigotry.

Over the years, many of us have raised concerns about how your platform may have a negative impact on our communities, with disappointing results. For example, we have requested that you address attacks on African Americans and Muslims, organizing by hate groups, and the censorship of Black, Arab, Muslim, and other marginalized voices. As a result of the pervasive presence and organizing by hate groups on your platform—some could not exist as national level entities without it—we have repeatedly requested that you convene a gathering with civil rights organizations to discuss appropriate and strategic responses. While you were unable to sufficiently respond to the concerns raised above, Facebook participated in and organized events that stigmatized Muslims and other communities such as a recent convening called "Tech Against Terrorism."

Though in the past you have displayed a willingness to listen to our concerns, we have yet to see meaningful change. It is our hope that recent developments will mark a new chapter in Facebook's commitment to protecting the rights of all who use your platform.

As we continue this important dialogue, we urge you to:

1. Fully disclose to the public all of the ads, pages, events, accounts, and posts you have traced back to Russian operatives targeting African American, LGBTQ, and Muslim communities. In particular, we believe that Facebook has a special responsibility to notify those individuals and organizations who have been impersonated or misrepresented.
2. Bring on an independent third-party team to conduct a thorough and public audit of the civil rights impact of your policies and programs, as well as how the platform has been used by hate groups, political entities, and others to stoke racial or religious resentment or violence. Other leading companies in the

---

<sup>10</sup> Facebook "About" page, February 4, 2004, available at [https://www.facebook.com/pg/facebook/about/?ref=page\\_internal](https://www.facebook.com/pg/facebook/about/?ref=page_internal).

Facebook, Inc  
October 30, 2017  
Page 4 of 5

industry like Airbnb have made the decision to conduct such an assessment, and we hope you will follow their lead.

3. Regularly convene a new working group of a diverse group of civil rights organizations working to counter bigotry, and solicit input on policies and processes from this group. And, integrate addressing hate into Facebook's corporate structure by:
  - a. Assigning a board committee with responsibility for assessing management efforts to stop hate groups, state actors, and individuals engaged in hate from using your platform and tools;
  - b. Assigning a senior manager who is a member of Facebook's Executive Team with authority to oversee addressing hate company-wide and name that person publicly and employing staff with expertise in this area to vet advertisements and develop process and procedures the address this issue; and,
  - c. Creating a committee of outside advisors with expertise in identifying and tracking hate who will be responsible for producing an annual report on the effectiveness of steps taken by Facebook.
4. Develop, with input from diverse civil rights groups and experts, and make public a clear process for how Facebook:
  - a. Reviews content constituting hate speech;
  - b. Reviews efforts to use Facebook as a platform to stoke identity-based, racial, or religious resentment or violent actions; and,
  - c. Responds to complaints about content that reasonably creates fear and chills speech on Facebook.
5. Make public detailed information regarding training and support for anti-immigrant, anti-Muslim, anti-black, and anti-LGBTQ organizations, including the monetary value of these services; and establish a fund to provide grants to organizations combating hatred and bigotry.

Thank you in advance for your consideration. Please contact Naheed Qureshi at [naheed@muslimadvocates.org](mailto:naheed@muslimadvocates.org) with any questions.

We look forward to your reply.

Sincerely,

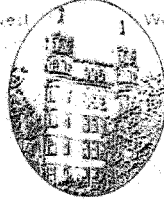
Arab American Institute (AAI)  
Asian Americans Advancing Justice | AAJC  
Center for Media Justice

Facebook, Inc  
October 30, 2017  
Page 5 of 5

Center for New Community  
Color of Change  
CREDO  
Human Rights Campaign (HRC)  
The Leadership Conference on Civil and Human Rights  
League of United Latin American Citizens (LULAC)  
MoveOn.org  
Muslim Advocates  
NAACP  
NAACP Legal Defense and Educational Fund, Inc. (LDF)  
National Center for Lesbian Rights  
National Hispanic Media Coalition  
National LGBTQ Task Force  
National Sikh Campaign  
Sikh Coalition  
Southern Poverty Law Center

NATIONAL COUNCIL OF NEGRO WOMEN, INC.

635 Pennsylvania Avenue, Northwest Washington, DC 20004 202-737-0120



(202) 737-0120

April 10, 2018

NCNW is an organization comprised of 32 national women's organizations and 200 community-based sections, with a combined reach of more than 2,000,000 women and men. One of NCNW's "Four for the Future" priorities is advocating for sound public policy and this requires that we stay vigilant about those issues that impact our communities.

We may never know for sure the extent to which the actions of Facebook, Cambridge Analytica or Palantir contributed to a sharp decline in black voter turnout (from 66% to 60%) between 2012 and 2016. What we do know is fairly straightforward.

Wittingly or not, it is likely that the Facebook permitted the most popular social media platform in the world to be weaponized against its users. The result is a weakening of democratic values and institutions. When Mr. Zuckerberg testifies before the House Committee on Energy and Commerce this week, the most important questions pertain to the future. We encourage NCNW members and the members of Congress to enact policy solutions in response to these questions:

1. What is the tech industry doing now to protect users' privacy?
2. What regulations should Congress enact to protect the American electorate from interference in future elections?
3. What will Facebook do to help restore confidence in social media and rectify the damage that has been done?

NCNW's mission is to lead, advocate for and empower women of African descent, their families and communities. Access to high quality public education, judicial appointments, census and redistricting, consumer finance protection, access to affordable health care, police use of force, criminal justice reform, environmental protection affect all Americans, but are of particular significance to the black community. Each of these issues is framed by federal public policy.

Citizens must assure that industry and policy makers alike understand that in our system of government, political clout is a currency as valuable as economic wealth. Proven threats to either demand protection and restoration.

Take action, Contact your member of Congress today with this simple message: Protect our privacy and our votes.

  
Janice L. Mathis

GREG WALDEN, OREGON  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115

Majority (201) 225-3927  
Minority (202) 225-3641

May 14, 2018

Mr. Mark Zuckerberg  
Chairman and CEO  
Facebook, Inc.  
1 Hacker Way  
Menlo Park, CA 94025


Dear Mr. Zuckerberg:

Thank you for appearing before the Committee on Energy and Commerce on Wednesday, April 11, 2018, to testify at the hearing entitled "Facebook: Transparency and Use of Consumer Data."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions by the close of business on Friday, June 29, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to [ali.fulling@mail.house.gov](mailto:ali.fulling@mail.house.gov).

Thank you again for your time and effort preparing and delivering testimony before the Committee.

Sincerely,



Greg Walden  
Chairman

cc: Frank Pallone, Ranking Member

Attachment

[Questions submitted for the record and responses from Facebook, Inc., are saved in committee records and are available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108090>.]