

FOSTERING A HEALTHIER INTERNET TO PROTECT CONSUMERS

JOINT HEARING

BEFORE THE
SUBCOMMITTEE ON COMMUNICATIONS AND
TECHNOLOGY
AND THE
SUBCOMMITTEE ON CONSUMER PROTECTION AND
COMMERCE
OF THE
COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

—————
OCTOBER 16, 2019
—————

Serial No. 116-69



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

—————
U.S. GOVERNMENT PUBLISHING OFFICE

43-533 PDF

WASHINGTON : 2021

COMMITTEE ON ENERGY AND COMMERCE

FRANK PALLONE, JR., New Jersey
Chairman

BOBBY L. RUSH, Illinois	GREG WALDEN, Oregon
ANNA G. ESHOO, California	<i>Ranking Member</i>
ELIOT L. ENGEL, New York	FRED UPTON, Michigan
DIANA DeGETTE, Colorado	JOHN SHIMKUS, Illinois
MIKE DOYLE, Pennsylvania	MICHAEL C. BURGESS, Texas
JAN SCHAKOWSKY, Illinois	STEVE SCALISE, Louisiana
G. K. BUTTERFIELD, North Carolina	ROBERT E. LATTA, Ohio
DORIS O. MATSUI, California	CATHY McMORRIS RODGERS, Washington
KATHY CASTOR, Florida	BRETT GUTHRIE, Kentucky
JOHN P. SARBANES, Maryland	PETE OLSON, Texas
JERRY McNERNEY, California	DAVID B. McKINLEY, West Virginia
PETER WELCH, Vermont	ADAM KINZINGER, Illinois
BEN RAY LUJAN, New Mexico	H. MORGAN GRIFFITH, Virginia
PAUL TONKO, New York	GUS M. BILIRAKIS, Florida
YVETTE D. CLARKE, New York, <i>Vice Chair</i>	BILL JOHNSON, Ohio
DAVID LOEB SACK, Iowa	BILLY LONG, Missouri
KURT SCHRADER, Oregon	LARRY BUCSHON, Indiana
JOSEPH P. KENNEDY III, Massachusetts	BILL FLORES, Texas
TONY CARDENAS, California	SUSAN W. BROOKS, Indiana
RAUL RUIZ, California	MARKWAYNE MULLIN, Oklahoma
SCOTT H. PETERS, California	RICHARD HUDSON, North Carolina
DEBBIE DINGELL, Michigan	TIM WALBERG, Michigan
MARC A. VEASEY, Texas	EARL L. "BUDDY" CARTER, Georgia
ANN M. KUSTER, New Hampshire	JEFF DUNCAN, South Carolina
ROBIN L. KELLY, Illinois	GREG GIANFORTE, Montana
NANETTE DIAZ BARRAGÁN, California	
A. DONALD McEACHIN, Virginia	
LISA BLUNT ROCHESTER, Delaware	
DARREN SOTO, Florida	
TOM O'HALLERAN, Arizona	

PROFESSIONAL STAFF

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

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

MIKE DOYLE, Pennsylvania
Chairman

JERRY McNERNEY, California	ROBERT E. LATTA, Ohio
YVETTE D. CLARKE, New York	<i>Ranking Member</i>
DAVID LOEBSACK, Iowa	JOHN SHIMKUS, Illinois
MARC A. VEASEY, Texas	STEVE SCALISE, Louisiana
A. DONALD McEACHIN, Virginia	PETE OLSON, Texas
DARREN SOTO, Florida	ADAM KINZINGER, Illinois
TOM O'HALLERAN, Arizona	GUS M. BILIRAKIS, Florida
ANNA G. ESHOO, California	BILL JOHNSON, Ohio
DIANA DeGETTE, Colorado	BILLY LONG, Missouri
G. K. BUTTERFIELD, North Carolina	BILL FLORES, Texas
DORIS O. MATSUI, California, <i>Vice Chair</i>	SUSAN W. BROOKS, Indiana
PETER WELCH, Vermont	TIM WALBERG, Michigan
BEN RAY LUJAN, New Mexico	GREG GIANFORTE, Montana
KURT SCHRADER, Oregon	GREG WALDEN, Oregon (<i>ex officio</i>)
TONY CARDENAS, California	
DEBBIE DINGELL, Michigan	
FRANK PALLONE, JR., New Jersey (<i>ex officio</i>)	

SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE

JAN SCHAKOWSKY, Illinois
Chairwoman

KATHY CASTOR, Florida	CATHY McMORRIS RODGERS, Washington
MARC A. VEASEY, Texas	<i>Ranking Member</i>
ROBIN L. KELLY, Illinois	FRED UPTON, Michigan
TOM O'HALLERAN, Arizona	MICHAEL C. BURGESS, Texas
BEN RAY LUJAN, New Mexico	ROBERT E. LATTA, Ohio
TONY CARDENAS, California, <i>Vice Chair</i>	BRETT GUTHRIE, Kentucky
LISA BLUNT ROCHESTER, Delaware	LARRY BUCSHON, Indiana
DARREN SOTO, Florida	RICHARD HUDSON, North Carolina
BOBBY L. RUSH, Illinois	EARL L. "BUDDY" CARTER, Georgia
DORIS O. MATSUI, California	GREG GIANFORTE, Montana
JERRY McNERNEY, California	GREG WALDEN, Oregon (<i>ex officio</i>)
DEBBIE DINGELL, Michigan	
FRANK PALLONE, JR., New Jersey (<i>ex officio</i>)	

C O N T E N T S

	Page
Hon. Mike Doyle, a Representative in Congress from the Commonwealth of Pennsylvania, opening statement	2
Prepared statement	3
Hon. Robert E. Latta, a Representative in Congress from the State of Ohio, opening statement	4
Prepared statement	5
Hon. Jan Schakowsky, a Representative in Congress from the State of Illinois, opening statement	6
Prepared statement	8
Hon. Cathy McMorris Rodgers, a Representative in Congress from the State of Washington, opening statement	8
Prepared statement	10
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	11
Prepared statement	12
Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement	13
Prepared statement	15
Hon. Anna G. Eshoo, a Representative in Congress from the State of California, prepared statement	125

WITNESSES

Steve Huffman, Cofounder and Chief Executive Officer, Reddit, Inc.	17
Prepared statement	20
Answers to submitted questions	232
Danielle Keats Citron, Professor of Law, Boston University School of Law	24
Prepared statement	26
Answers to submitted questions	242
Corynne McSherry, Ph.D., Legal Director, Electronic Frontier Foundation	37
Prepared statement	39
Answers to submitted questions	253
Gretchen Peters, Executive Director, Alliance to Counter Crime Online	57
Prepared statement	59
Answers to submitted questions	262
Katherine Oyama, Global Head of Economic Property Policy, Google	65
Prepared statement	67
Answers to submitted questions	269
Hany Farid, Ph.D., Professor, University of California, Berkeley	77
Prepared statement	79
Answers to submitted questions	284

SUBMITTED MATERIAL

Letter of October 15, 2021, from Carl Szabo, Vice President and General Counsel, NetChoice, to subcommittee members, bmitted by Mr. McNerney ...	126
Statement of the Electronic Frontier Foundation, "Could Platform Safe Harbors Save the NAFTA Talks?," January 23, 2018, submitted by Mr. Bili-rakis	147

VI

	Page
Letter of October 14, 2019, from Ruth Vitale, Chief Executive Officer, CreativeFuture, to Mr. Pallone and Mr. Walden, submitted by Ms. Schakowsky ¹	
Letter of October 16, 2021, from Chip Rogers, President and Chief Executive Officer, American Hotel & Lodging Association, to Mr. Pallone and Mr. Walden, submitted by Ms. Schakowsky	150
Letter, undated, from Michael Petricone, Senior Vice President, Consumer Technology Association, to Mr. Pallone, et al., submitted by Ms. Schakowsky	152
Letter of September 9, 2019, from Steve Shur, President, The Travel Technology Association, to Mr. Pallone, et al., submitted by Ms. Schakowsky	155
Statement of Airbnb, “Airbnb & the Communications Decency Act Section 230,” submitted by Ms. Schakowsky	158
Letter of October 15, 2019, from James P. Steyer, Founder and Chief Executive Officer, Common Sense Media, to Mr. Pallone and Mr. Walden, submitted by Ms. Schakowsky	160
Letter of October 15, 2019, from the Computer & Communications Industry Association, et al., to Mr. Pallone, et al., submitted by Ms. Schakowsky	164
Letter of October 16, 2019, from Hon. Ed Case, a Representative in Congress from the State of Hawaii, to Mr. Doyle, et al., submitted by Ms. Schakowsky	166
Letter of October 10, 2019, from American Family Voices, et al., to Members of Congress, submitted by Ms. Schakowsky	169
Statement of the Internet Infrastructure Coalition, October 16, 2019, submitted by Ms. Schakowsky	171
Letter of May 3, 2019, from Hon. Steve Daines, a U.S. Senator from the State of Montana, and Mr. Gianforte, to Sundar Pichai, Chief Executive Officer, Google, submitted by Ms. Schakowsky	174
Letter of October 15, 2019, from Berin Szóka, President, TechFreedom, to Mr. Pallone and Mr. Walden, submitted by Ms. Schakowsky	175
Letter of October 16, 2019, from Michael Beckerman, President and Chief Executive Officer, the Internet Association, to Mr. Pallone and Mr. Walden, submitted by Ms. Schakowsky	190
Letter of October 15, 2019, from the Wikimedia Foundation to Mr. Pallone, et al., submitted by Ms. Schakowsky	192
Statement of the Motion Picture Association, Inc., by Neil Fried, Senior Vice President and Senior Counsel, October 16, 2019, submitted by Ms. Schakowsky	196
Article of September 7, 2017, “Searching for Help: She turned to Google for help getting sober. Then she had to escape a nightmare,” by Carl Ferguson, The Verge, submitted by Ms. Schakowsky	199
Statement of R Street Institute by Jeffrey Westling, Fellow, Technology and Innovation, et al., October 16, 2019, submitted by Ms. Schakowsky	217

¹The letter has been retained in committee files and also is available at <https://docs.house.gov/meetings/IF/IF16/20191016/110075/HHRG-116-IF16-20191016-SD005.pdf>.

FOSTERING A HEALTHIER INTERNET TO PROTECT CONSUMERS

WEDNESDAY, OCTOBER 16, 2019

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY
JOINT WITH THE
SUBCOMMITTEE ON CONSUMER PROTECTION AND
COMMERCE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittees met, pursuant to notice, at 10:02 a.m., in the John D. Dingell Room 2123, Rayburn House Office Building, Hon. Mike Doyle (chairman of the Subcommittee on Communications and Technology) and Hon. Jan Schakowsky (chairwoman of the Subcommittee on Consumer Protection and Commerce) presiding.

Members present: Representatives Doyle, Schakowsky, Eshoo, DeGette, Matsui, Castor, McNerney, Welch, Clarke, Loebsack, Schrader, Cárdenas, Dingell, Veasey, Kelly, Blunt Rochester, Soto, O'Halleran, Pallone (ex officio), Latta (Subcommittee on Communications and Technology ranking member), Rodgers (Subcommittee on Consumer Protection and Commerce ranking member), Shimkus, Burgess, Guthrie, Kinzinger, Bilirakis, Johnson, Bucshon, Brooks, Hudson, Walberg, Carter, Gianforte, and Walden (ex officio).

Staff present: AJ Brown, Counsel; Jeffrey C. Carroll, Staff Director; Sharon Davis, Chief Clerk; Parul Desai, FCC Detailee; Evan Gilbert, Deputy Press Secretary; Lisa Goldman, Senior Counsel; Tiffany Guarascio, Deputy Staff Director; Alex Hoehn-Saric, Chief Counsel, Communications and Consumer Protection; Zach Kahan, Outreach and Member Service Coordinator; Jerry Leverich, Senior Counsel; Dan Miller, Senior Policy Analyst; Phil Murphy, Policy Coordinator; Joe Orlando, Executive Assistant; Alivia Roberts, Press Assistant; Tim Robinson, Chief Counsel; Chloe Rodriguez, Policy Analyst; Andrew Souvall, Director of Communications, Outreach, and Member Services; Sydney Terry, Policy Coordinator; Rebecca Tomilchik, Staff Assistant; Mike Bloomquist, Minority Staff Director; Michael Engel, Minority Detailee, Communications and Technology; Bijan Koochmaraie, Minority Deputy Chief Counsel, Consumer Protection and Commerce; Tim Kurth, Minority Deputy Chief Counsel, Communications and Technology; Brannon Rains, Minority Legislative Clerk; Evan Viau, Minority Professional Staff Member, Communications and Technology; and Nate Wilkins, Minority Fellow, Communications and Technology.

Mr. DOYLE. The committee will now come to order. The Chair now recognizes himself for 5 minutes for an opening statement.

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

Online content moderation has largely enabled the internet experience that we know today. Whether it is looking up restaurant reviews on Yelp, catching up on “SNL” on YouTube, or checking in on a friend or a loved one on social media, these are all experiences that we have come to know and rely on. And the platforms we go to to do these things have been enabled by user-generated content as well as the ability of these companies to moderate that content and create communities.

Section 230 of the Communications Decency Act has enabled that ecosystem to evolve. By giving online companies the ability to moderate content without equating them to the publisher or speaker of that content, we have enabled the creation of massive online communities of millions and billions of people to come together and interact.

Today, this committee will be examining that world that Section 230 has enabled, both the good and the bad.

I would like to thank the witnesses for appearing before us today. Each of you represents important perspectives related to the content moderation and the online ecosystem.

Many of you bring up complex concerns in your testimony, and I agree that this is a complex issue. I know that some of you have argued that Congress should amend 230 to address things such as online criminal activity, disinformation, and hate speech, and I agree these are serious issues.

Like too many other communities, my hometown of Pittsburgh has seen what unchecked hate can lead to. Almost a year ago, our community suffered the most deadly attack on Jewish Americans in our Nation’s history. The shooter did so after posting a series of anti-Semitic remarks on a fringe site before finally posting that he was “going in.”

A similar attack occurred in New Zealand, and the gunman streamed his despicable acts on social media sites. And while some of these sites moved to quell that spread of that content, many didn’t move fast enough, and the algorithms meant to help sports highlights and celebrity selfies go viral helped amplify a heinous act.

In 2016, we saw similar issues when foreign adversaries used the power of these platforms against us to disseminate disinformation and foment doubt in order to sow division and instill distrust in our leaders and institutions.

Clearly, we all need to do better, and I would strongly encourage the witnesses before us that represent these online platforms and other major platforms to step up.

The other witnesses on the panel bring up serious concerns with the kind of content available on your platforms and the impact that content is having on society. And as they point out, some of those impacts are very disturbing. You must do more to address these concerns.

That being said, Section 230 doesn't just protect the largest platforms or the most fringe websites. It enables comment sections on individual blogs, people to leave honest and open reviews, and free and open discussion about controversial topics.

The kind of ecosystem that has been enabled by more open online discussions has enriched our lives and our democracy. The ability of individuals to have voices heard, particularly marginalized communities, cannot be understated. The ability of people to post content that speaks truth to power has created political movements in this country and others that have changed the world we live in. We all need to recognize the incredible power this technology has for good as well as the risks we face when it is misused.

I want to thank you all again for being here, and I look forward today to our discussion.

[The prepared statement of Mr. Doyle follows:]

PREPARED STATEMENT OF HON. MIKE DOYLE

Online content moderation has largely enabled the internet experience we know today. Whether it's looking up restaurant reviews on Yelp, catching up on S-N-L on YouTube, or checking in on a friend or loved one on social media, these are all experiences we have come to rely on.

And the platforms we go to do these things have been enabled by user-generated content, as well as the ability of these companies to moderate that content and create communities.

Section 230 of the Communications Decency Act has enabled that ecosystem to evolve.

By giving online companies the ability to moderate content without equating them to the publisher or speaker of that content, we've enabled the creation of massive online communities of millions and billions of people who can come together and interact.

Today, this committee will be examining the world that Section 230 has enabled—both the good and the bad.

I'd like to thank the witnesses for appearing before us today. Each of you represents important perspectives related to content moderation in the online ecosystem. Many of you bring up complex concerns in your testimony, and I agree that this is a complicated issue.

I know some of you have argued that Congress should amend 230 to address things such as online criminal activity, disinformation, and hate speech; and I agree that these are serious issues.

Like too many other communities, my hometown of Pittsburgh has seen what unchecked hate can lead to.

Almost a year ago, our community suffered the most deadly attack on Jewish Americans in our nation's history; the shooter did so after posting a series of anti-Semitic remarks on a fringe site before finally posting that he was "going in."

A similar attack occurred in New Zealand, and the gunman streamed his despicable acts on social media sites. And while some of these sites moved to quell the spread of this content, many didn't move fast enough. And the algorithms meant to help sports highlights and celebrity selfies go viral helped amplify a heinous act.

In 2016, we saw similar issues, when foreign adversaries used the power of these platforms against us to disseminate disinformation and foment doubt in order to sow division and instill distrust in our leaders and institutions.

Clearly, we all need to do better, and I would strongly encourage the witnesses before us who represent online platforms and other major platforms to step up.

The other witnesses on the panel bring up serious concerns with the kinds of content available on your platforms and the impact that content is having on our society. And as they point out, some of those impacts are very disturbing. You must do more to address these concerns.

That being said, Section 230 doesn't just protect the largest platforms or the most fringe websites.

It enables comment sections on individual blogs, honest and open reviews of goods and services, and free and open discussion about controversial topics.

It has enabled the kind of ecosystem that, by producing more open online discussions, has enriched our lives and our democracy.

The ability of individuals to have their voices heard, particularly marginalized communities, cannot be understated.

The ability of people to post content that speaks truth to power has created political movements in this country and others that have changed the world we live in.

We all need to recognize the incredible power this technology has had for good, as well as the risks we face when it's misused.

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

I yield 1 minute to my good friend Ms. Matsui.

Mr. DOYLE. And I would now like to yield the balance of my time to my good friend, Ms. Matsui.

Ms. MATSUI. Thank you, Mr. Chairman.

I want to thank the witnesses for being here today.

In April 2018, Mark Zuckerberg came before Congress and said, "It was my mistake, and I am sorry" when pushed about Facebook's role in allowing Russia to influence the 2016 Presidential election.

Fast forward 555 days. I fear that Mr. Zuckerberg may not have learned from his mistake. Recent developments confirm what we have all feared. Facebook will continue to allow ads that push falsehoods and lies, once again making its online ecosystem fertile ground for election interference in 2020.

The decision to remove blatantly false information should not be a difficult one. The choice between deepfakes, hate speech, online bullies, and a fact-driven debate should be easy. If Facebook doesn't want to play referee about the truth in political speech, then they should get out of the game.

I hope this hearing produces a robust discussion, because we need it now more than ever.

Mr. Chairman, I yield back. Thank you.

Mr. DOYLE. Thank you. The gentlelady yields back.

The Chair now recognizes Mr. Latta, the ranking member for the subcommittee, for 5 minutes for his opening statement.

**OPENING STATEMENT OF HON. ROBERT E. LATTA, A
REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO**

Mr. LATTA. Well, thank you, Mr. Chairman, for holding today's hearing.

And thank you very much to our witnesses for appearing before us. And, again, welcome to today's hearing on content moderation and a review of Section 230 of the Communications Decency Act.

This hearing is a continuation of a serious discussion we began last session as to how Congress should examine the law and ensure accountability and transparency for the hundreds of millions of Americans using the internet today.

We have an excellent panel of witnesses that represent a balanced group of stakeholders who perform work closely tied to Section 230. They range from large to small companies as well as academics and researchers.

Let me be clear: I am not advocating that Congress repeal the law, nor am I advocating that Congress consider niche carveouts that could lead to a slippery slope of the death by a thousand cuts that some have argued would upend the internet industry if the law was entirely repealed.

But before we discuss whether or not Congress should make modest, nuanced modifications to the law, we should first understand how we got to this point. It is important to look at Section 230 in context and when it was written. At the time, the decency portion of the Telecom Act of 1996 included other prohibitions on objectionable or lewd content that polluted the early internet. Provisions that were written to target obscene content were ultimately struck down by the Supreme Court, but the Section 230 provisions remained.

Notably, CDA 230 was intended to encourage internet platforms that interact with computer services like CompuServe and America Online to proactively take down offensive content. As Chris Cox stated on the House floor, “We want to encourage people like Prodigy, like CompuServe, like America Online, like the new Microsoft Network, to do everything possible for us, the consumer, to help us control, at the portals of our computer, at the front door of our house, what comes in and what our children see.”

It is unfortunate, however, that the courts took such a broad interpretation of Section 230, simply granting a broad liability protection without platforms having to demonstrate that they are doing, quote, “everything possible.” Instead of encouraging use of the sword that Congress envisioned, numerous platforms have hidden behind the shield and use procedural tools to avoid litigation without having to take the responsibility.

Not only are Good Samaritans sometimes being selective in taking down harmful or illegal activity, but Section 230 has been interpreted so broadly that bad Samaritans can skate by without accountability.

That is not to say all platforms never use the tools afforded by Congress. Many do great things. Many of the bigger platforms remove billions, and that is with a “b,” accounts annually. But oftentimes these instances are the exception, not the rule.

Today we will dig deeper into those examples and learn how platforms decide to remove content, whether it is with the tools provided by Section 230 or with their own self-constructed terms of service. Under either authority, we should be encouraging enforcement to continue.

Mr. Chairman, I thank you for holding this important hearing so that we can have an open discussion on Congress’ intent of CDA 230 and if we should reevaluate the law. We must ensure that platforms are held reasonably accountable for activity on their platform without drastically affecting the innovative startups.

And with that, Mr. Chairman, I yield back the balance of my time.

[The prepared statement of Mr. Latta follows:]

PREPARED STATEMENT OF HON. ROBERT E. LATTA

Welcome to today’s hearing on content moderation and a review of Section 230 of the Communications Decency Act. This hearing is a continuation of a serious discussion we began last session as to how Congress should examine the law and ensure accountability and transparency for the hundreds of millions of Americans using the internet today.

We have an excellent panel of witnesses that represent a balanced group of stakeholders who perform work closely tied to Section 230—this well-respected group ranges from big companies to small companies, as well as academics to researchers.

Let me be clear, I am not advocating that Congress repeal the law. Nor am I advocating for Congress to consider niche “carveouts” that could lead to a slippery slope of the “death-by-a-thousand-cuts” that some have argued would upend the internet industry as if the law were repealed entirely. But before we discuss whether or not Congress should make modest, nuanced modifications to the law, we first should understand how we’ve gotten to this point.

It’s important to take Section 230 in context of when it was written. At the time, the “decency” portion of the Telecom Act of 1996 included other prohibitions on objectionable or lewd content that polluted the early internet. Provisions that were written to target obscene content were ultimately struck down at the Supreme Court, but the Section 230 provisions remained.

Notably, CDA 230 was intended to encourage internet platforms—then, “interactive computer services” like CompuServe and America Online—to proactively take down offensive content. As Chris Cox stated on the floor of the House, “We want to encourage people like Prodigy, like CompuServe, like America Online, like the new Microsoft Network, to do everything possible for us, the customer, to help us control, at the portals of our computer, at the front door of our house, what comes in and what our children see.”

It is unfortunate, however, that the courts took such a broad interpretation of Section 230, simply granting broad liability protection without platforms having to demonstrate that they are doing, quote, “everything possible.” Instead of encouraging use of the sword that Congress envisioned, numerous platforms have hidden behind the shield and used procedural tools to avoid litigation without having to take any responsibility. Not only are “Good Samaritans” sometimes being selective in taking down harmful or illegal activity, but Section 230 has been interpreted so broadly that “bad Samaritans” can skate by without accountability, too.

That’s not to say all platforms never use the tools afforded them by Congress; many do great things. Some of the bigger platforms remove billions—with a B—accounts annually. But oftentimes, these instances are the exception, not the rule. Today we will dig deeper into those examples to learn how platforms decide to remove content—whether it’s with the tools provided by Section 230 or with their own self-constructed terms of service. Under either authority, we should be encouraging enforcement to continue.

Mr. Chairman, I thank you for holding this important hearing so that we can have an open discussion on Congress’ intent of CDA 230 and if we should reevaluate the law. We must ensure platforms are held reasonably accountable for activity on their platform, without drastically affecting innovative startups.

Thank you, I yield back.

Mr. DOYLE. The gentleman yields back.

I should have mentioned this is a joint hearing between our committee and the Committee on Consumer Protection and Commerce. And I would like to recognize the chair of that committee for 5 minutes, Ms. Schakowsky.

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

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

And good morning, and thank all the panelists for being here today.

The internet certainly has improved our lives in many, many ways and enabled Americans to more actively participate in society, education, and commerce.

Section 230 of the Communications Decency Act has been at the heart of the United States’ internet policy for over 20 years. Many say that this law allowed free speech to flourish, allowing the internet to grow into what it is today.

In the early days of the internet, it was intended to encourage online platforms to moderate user-generated content, to remove offensive, dangerous, or illegal content.

The internet has come a long way since the law was first enacted. The amount and sophistication of user postings has increased exponentially.

Unfortunately, the number of Americans who report experiencing extremism, extreme online harassment, which includes sexual harassment, stalking, bullying, and threats of violence, have gone up. Over the last 2 years, 37 percent of users say that they have experienced that this year. Likewise, extremism, hate speech, election interference, and other problematic content is proliferating.

The spread of such content is problematic, that is for sure, and actually causes some real harm that multibillion-dollar companies like Facebook, Google, and Twitter can't or won't fix.

And if this weren't enough cause for concern, more for-profit businesses are attempting to use Section 230 as a liability shield actively, that they have nothing to do with third-party content or content moderation policy.

In a recent Washington Post article, Uber executives seemed to be opening the door to claiming vast immunity from labor, criminal, and local traffic liability based on Section 230. This would represent a major unraveling of 200 years of social contracts, community governance, and congressional intent.

Also at issue is the Federal Trade Commission's Section 5 authority on unfair or deceptive practices. The FTC pursues Section 5 cases on website-generated content, but the terms of service violations for third-party content may also be precluded by the 230 immunity.

I wanted to talk a bit about injecting 230 into trade agreements. It seems to me that we have already seen that now in the Japan trade agreement, and there is a real push to include that now in the Mexico-Canada-U.S. trade agreement. There is no place for that. I think that the laws in these other countries don't really accommodate what the United States has done about 230.

The other thing is, we are having a discussion right now, an important conversation about 230, and in the midst of that conversation, because of all the new developments, I think it is just inappropriate right now at this moment to insert this liability protection into trade agreements.

As a member of the working group that is helping to negotiate that agreement, I am pushing hard to make sure that it just isn't there. I don't think we need to have any adjustment to 230. It just should not be in trade agreements.

So all of the issues that we are talking about today indicate that there may be a larger problem that 230 no longer is achieving the goal of encouraging platforms to protect their users. And today I hope that we can discuss holistic solutions, not talking about eliminating 230 but having a new look at that in the light of the many changes that we are seeing into the world of big tech right now.

I look forward to hearing from our witnesses and how it can be made even better for consumers.

And I yield back. Thank you.

[The prepared statement of Ms. Schakowsky follows:]

PREPARED STATEMENT OF HON. JAN SCHAKOWSKY

Good morning, and thank you all for attending today's hearing. The internet has improved our lives in many ways and enabled Americans to more actively participate in society, education, and commerce.

Section 230 of the Communications Decency Act has been at the heart of the United States' internet policy for over 20 years. Many say that this law allowed free speech to flourish, allowing the internet to grow into what it is today. In the early days of the internet, it was intended to encourage online platforms to moderate user-generated content—to remove offensive, dangerous, or illegal content.

The internet has come a long way since the law was enacted. The amount and sophistication of user posts have increased exponentially. Unfortunately the number of Americans who report experiencing extreme online harassment, which includes sexual harassment, stalking, bullying, and threats of violence, has gone up over the last two years. Likewise, extremism, hate speech, election inference, and other problematic content is proliferating.

The spread of such content is a problem that multibillion-dollar companies—like Facebook, Google, and Twitter—can't or won't fix.

As if this weren't enough cause for concern, more for-profit businesses are attempting to use section 230 as a liability shield for activities that have nothing to do with 3rd party content or content moderation policies.

In a recent Washington Post article, Uber executives seem to be opening the door to claiming vast immunity from labor, criminal, and local traffic liability based on section 230. This would represent a major unraveling of 200 years of social contracts, community governance, and Congressional intent.

Also at issue is the Federal Trade Commission's Section 5 authority on unfair or deceptive practices. The FTC has pursued Section 5 cases on website-generated content, but terms of service violations for third-party content may also be precluded by the 230 immunity.

Lastly, this committee must consider the effects of including 230 language in trade agreements. Today we are having a thoughtful discussion about 230 to ensure we find the right balance between protecting free speech, protecting Americans from violence and harassment online, and ensuring that multibillion-dollar companies can be held accountable to consumers. It strikes me as premature to export our own political debate on 230 to our trading partners, while at the same time limiting Congress' ability to have said debate.

Each of the issues I mentioned are indications that there may be a larger problem, that 230 may no longer be achieving the goal of encouraging platforms to protect their users. Today, I hope we can discuss holistic solutions.

The internet has provided many benefits to our society, and I look forward to hearing from our witnesses how it can be made even better for consumers.

Mr. DOYLE. The gentlelady yields back.

The Chair now recognizes the ranking member of the committee, Mrs. McMorris Rodgers.

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

Mrs. RODGERS. Good morning. Welcome to today's joint hearing on online content management.

As the Republican leader on the Consumer Protection and Commerce Subcommittee, it is my priority to protect consumers while preserving the ability for small businesses and startups to innovate. In that spirit, today we are discussing online platforms in Section 230 of the Communications Decency Act.

In the early days of the internet, two companies were sued for content posted on their website by users. One company sought to moderate content on their platform; the other did not. In deciding these cases, the Court found the company that did not make any content decisions was immune from liability, but the company that moderated content was not.

It was after these decisions that Congress created Section 230. Section 230 is intended to protect, quote, “interactive computer services” from being sued over what users post while also allowing them to moderate content that may be harmful, illicit, or illegal.

This liability protection has played a critical and important role in the way we regulate the internet. It has allowed small businesses and innovators to thrive online without the fear of frivolous lawsuits from bad actors looking to make a quick buck.

Section 230 is also largely misunderstood. Congress never intended to provide immunity only to websites who are, quote, “neutral.” Congress never wanted platforms to simply be neutral conduits but, in fact, wanted platforms to moderate content. The liability protection also extended to allow platforms to make good-faith efforts to moderate material that is obscene, lewd, excessively violent, or harassing.

There is supposed to be a balance to the use of Section 230. Small internet companies enjoy a safe harbor to innovate and flourish online while also incentivizing companies to keep the internet clear of offensive and violent content by empowering these platforms to act and to clean up their own site.

The internet also revolutionized the freedom of speech by providing a platform for every American to have their voice heard and to access an almost infinite amount of information at their fingertips. Medium and other online blogs have provided a platform for anyone to write an op-ed. Wikipedia provides free, in-depth information on almost any topic you can imagine through mostly user-generated and moderated content. Companies that started in dorm rooms and garages are now global powerhouses.

We take great pride in being the global leader in tech and innovation. But while some of our biggest companies certainly have grown, have they matured? Today it is often difficult to go online without seeing harmful, disgusting, or somewhat illegal content.

To be clear, I fully support free speech and believe society strongly benefits from open dialogue and free expression online. I know that there have been some calls for Big Government to mandate or dictate free speech or ensure fairness online, and it is coming from both sides of the aisle.

Though I share similar concerns that others have expressed that are driving some of these policy proposals, I do not believe these proposals are consistent with the First Amendment. Republicans successfully fought to repeal the FCC’s Fairness Doctrine for broadcast regulation during the 1980s, and I strongly caution against advocating for a similar doctrine online.

It should not be the FCC, FTC, or any other Government agency’s job to moderate free speech online. Instead, we should continue to provide oversight of big tech and their use of Section 230 and encourage constructive discussions on the responsible use of content moderation.

This is a very important question that we are going to explore today with everyone on the panel. How do we ensure that companies with enough resources are responsibly earning their liability protection? We want companies to benefit not only from the shield but also use the sword Congress afforded them to rid their sites of harmful content.

I understand it is a delicate issue and certainly very nuanced. I want to be very clear: I am not for gutting Section 230. It is essential for consumers and entities in the internet ecosystem. Misguided and hasty attempts to amend or even repeal Section 230 for bias or other reasons could have unintended consequences for free speech and the ability for small businesses to provide new and innovative services.

But at the same time, it is clear we have reached a point where it is incumbent upon us as policymakers to have a serious and thoughtful discussion about achieving the balance on Section 230.

I thank you for the time, and I yield back.

[The prepared statement of Mrs. Rodgers follows:]

PREPARED STATEMENT OF HON. CATHY MCMORRIS RODGERS

Good morning and welcome to today's joint hearing on online content moderation. As the Republican Leader on the Consumer Protection and Commerce Subcommittee, it's my priority to protect consumers while preserving the ability for small business and startups to innovate.

In that spirit, today we are discussing online platforms and Section 230 of the Communications Decency Act.

In the early days of the internet, two companies were sued for content posted on their website by users.

One company sought to moderate content on their platform; the other did not.

In deciding these cases, the Court found the company that did not make any content decisions was immune from liability, but the company that moderated content was not.

It was after these decisions that Congress enacted Section 230.

Section 230 is intended to protect "interactive computer services" from being sued over what users post, while allowing them to moderate content that may be harmful, illicit, or illegal.

This liability protection has played a critically important role in the way we regulate the internet.

It's allowed small businesses and innovators to thrive online without fear of frivolous lawsuits from bad actors looking to make a quick buck.

Section 230 is also largely misunderstood. Congress never intended to provide immunity only to websites who are "neutral."

Congress never wanted platforms to simply be neutral conduits but—in fact—wanted platforms to moderate content.

The liability protection also extended to allow platforms to make good faith efforts to moderate material that is obscene, lewd, excessively violent, or harassing.

There is supposed to be a balance to the use of Section 230. Small internet companies enjoy a safe harbor to innovate and flourish online while also incentivizing companies to keep the internet clear of offensive and violent content by empowering these platforms to act and clean up their own site.

The internet has revolutionized the freedom of speech by providing a platform for every American to have their voice heard and to access an almost infinite amount of information at their fingertips.

Medium and other online blogs have provided a platform for anyone to write an op-ed.

Wikipedia provides free, in-depth information on almost any topic you can imagine, through mostly user-generated and moderated content.

Companies that started in dorm rooms and garages are now global powerhouses.

We take great pride in being the global leader in tech and innovation, but while some of our biggest companies certainly have grown, have they matured?

Today, it's often difficult to go online without seeing harmful, disgusting, and sometimes illegal content.

To be clear, I fully support free speech and believe society strongly benefits from open dialogue and free expression online.

I know there have been some calls for a Big Government mandate to dictate free speech or ensure fairness online—even coming from some of my colleagues on my side of the aisle.

Though I share similar concerns that others have expressed that are driving some of these policy proposals, I do not believe these proposals are consistent with the First Amendment.

Republicans successfully fought to repeal the FCC's Fairness Doctrine for broadcast regulation during the 1980s and I strongly caution against advocating for a similar doctrine online.

It should not be the FCC, FTC, or any Government agency's job to moderate free speech online.

Instead, we should continue to provide oversight of Big Tech and their use of Section 230 and encourage constructive discussions on the responsible use of content moderation.

This is an important question that we'll explore with our expert panel today: How do we ensure the companies with enough resources are responsibly earning their liability protection?

We want companies to benefit not only from the "shield" to liability, but also to use the "sword" Congress afforded them to rid their sites of harmful content.

I understand this is a delicate issue and certainly very nuanced.

I want to be very clear, I am not for gutting Section 230. It is essential for consumers and entities in the internet ecosystem.

Misguided and hasty attempts to amend or even repeal Section 230 for bias or other reasons could have disastrous, unintended consequences for free speech and the ability for small companies to provide new and innovative services.

At the same time, it is clear we have reached a point where it is incumbent upon policymakers to have a serious and thoughtful discussion about achieving the balance Section 230 is focused on:

Ensuring small businesses can innovate and grow, while also incentivizing companies to take more responsibility over their platforms.

Thank you. I yield back.

Mr. DOYLE. The gentlelady yields back.

The Chair now recognizes Mr. Pallone, chairman of the full committee, for 5 minutes for his opening statement.

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

Mr. PALLONE. Thank you, Chairman Doyle.

The internet is one of the single greatest human innovations. It promotes free expression, connections, and community. It also fosters economic opportunity, with trillions of dollars exchanged online every year.

One of the principal laws that paved the way for the internet to flourish is Section 230 of the Communications Decency Act, which, of course, passed as part of the Telecommunications Act of 1996. And we enacted this section to give platforms the ability to moderate their sites to protect consumers without excessive risk of litigation, and to be clear, Section 230 has been an incredible success.

But in the 20 years since Section 230 became law, the internet has become more complex and sophisticated. In 1996, the global internet reached only 36 million users, or less than 1 percent of the world's population. Only one in four Americans reported going online every day.

Compare that to now when nearly all of us are online almost every hour that we are not sleeping. Earlier this year, the internet passed 4.39 billion users worldwide. And here in the U.S., there are about 230 million smartphones that provide Americans instant access to online platforms. The internet has become a central part of our social, political, and economic fabric in a way that we couldn't have dreamed of when we passed the Telecommunications Act.

And with that complexity and growth, we also have seen the darker side of the internet grow. Online radicalization has spread, leading to mass shootings in our schools, churches, and movie thea-

ters. International terrorists are using the internet to groom recruits. Platforms have been used for the illegal sale of drugs, including those that sparked the opioid epidemic. Foreign governments and fraudsters have pursued political disinformation campaigns using new technology like deepfakes designed to sow civil unrest and disrupt democratic elections. And there are consent attacks against women, people of color, and other minority groups.

And perhaps most despicable of all is the growth in the horrendous sexual exploitation of children online. In 1998, there were 3,000 reports of material depicting the abuse of children online. Last year, 45 million photo and video reports were made. And while platforms are now better at detecting and removing this material, recent reporting shows that law enforcement officers are overwhelmed by the crisis.

And these are all issues that we can't ignore, and tech companies need to step up with new tools to help address these serious problems. Each of these issues demonstrates how online content moderation has not stayed true to the values underlying Section 230 and has not kept pace with the increasing importance of the global internet.

And there is no easy solution to keep this content off the internet. As policymakers, I am sure we all have our ideas about how we might tackle the symptoms of poor content moderation online while also protecting free speech, but we must seek to fully understand the breadth and depth of the internet today, how it has changed, and how it can be made better. We have to be thoughtful, careful, and bipartisan in our approach.

So it is with that in mind that I was disappointed that Ambassador Lighthizer, the U.S. Trade Representative, refused to testify today. The U.S. has included language similar to Section 230 in the United States-Mexico-Canada Agreement and the U.S.-Japan Trade Agreement.

Ranking Member Walden and I wrote to the Ambassador in August raising concerns about why the USTR has included this language in trade deals as we debate them across the Nation, and I was hoping to hear his perspective on why he believes that that was appropriate, because including provisions in trade agreements that are controversial to both Democrats and Republicans is not the way to get support from Congress, obviously. So hopefully the Ambassador will be more responsive to bipartisan requests in the future.

And with that, Mr. Chairman, I will yield back.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

The internet is one of the single greatest human innovations. It promotes free expression, connections, and community. It also fosters economic opportunity with trillions of dollars exchanged online every year.

One of the principal laws that paved the way for the internet to flourish is Section 230 of the Communications Decency Act, which passed as part of the Telecommunications Act of 1996. We enacted this section to give platforms the ability to moderate their sites to protect consumers, without excessive risk of litigation. And to be clear, Section 230 has been an incredible success.

But, in the 20 years since Section 230 became law, the internet has become more complex and sophisticated. In 1996, the global internet reached only 36 million users, or less than 1 percent of the world's population. Only one in four Americans

reported going online every day. Compare that to now, when nearly all of us are online almost every hour we are not sleeping. Earlier this year, the internet passed 4.39 billion users worldwide, and here in the U.S. there are about 230 million smartphones that provide Americans instant access to online platforms. The internet has become a central part of our social, political, and economic fabric in a way that we couldn't have dreamed of when we passed the Telecommunications Act.

And with that complexity and growth, we have also seen the darker side of the internet grow.

Online radicalization has spread, leading to mass shootings in our schools, churches, and movie theaters.

International terrorists are using the internet to groom recruits.

Platforms have been used for the illegal sale of drugs, including those that sparked the opioid epidemic.

Foreign governments and fraudsters have pursued political disinformation campaigns—using new technology like deepfakes—designed to sow civil unrest and disrupt democratic elections.

There are the constant attacks against women, people of color, and other minority groups.

And perhaps most despicable of all is the growth in the horrendous sexual exploitation of children online. In 1998, there were 3,000 reports of material depicting the abuse of children online. Last year, 45 million photo and video reports were made. While platforms are now better at detecting and removing this material, recent reporting shows that law enforcement officers are overwhelmed by this crisis.

These are all issues that cannot be ignored, and tech companies need to step up with new tools to help address these serious problems. Each of these issues demonstrates how online content moderation has not stayed true to the values underlying Section 230 and has not kept pace with the increasing importance of the global internet.

There is no easy solution to keep this content off the internet. As policymakers, I'm sure we all have our ideas about how we might tackle the symptoms of poor content moderation online while also protecting free speech.

We must seek to fully understand the breadth and depth of the internet today, how it has changed and how it can be made better. We must be thoughtful, careful, and bipartisan in our approach.

It is with that in mind that I am disappointed Ambassador Lighthizer, the United States Trade Representative (USTR), refused to testify today. The United States has included language similar to Section 230 in the United States-Mexico-Canada Agreement and the U.S.-Japan Trade Agreement. Ranking Member Walden and I wrote to the Ambassador in August raising concerns about why the USTR has included this language in trade deals as we debate them across the Nation, and I was hoping to hear his perspective on why he believes that is appropriate. Including provisions in trade agreements that are controversial to both Republicans and Democrats is not the way to get support from Congress. Hopefully, Ambassador Lighthizer will be more responsive to bipartisan requests in the future.

Mr. DOYLE. The gentleman yields back.

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

Oh.

Mr. WALDEN. Could mine be made part of it?

Mr. DOYLE. I apologize. The Chair now yields to my good friend, the ranking member, for 5 minutes.

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

Mr. WALDEN. How times have changed.

Thank you, Mr. Chairman.

And I want to welcome our witnesses today. Thank you for being here. It is really important work.

And I will tell you at the outset, we have got another subcommittee meeting upstairs, so I will be bouncing in between. But I have all your testimony and really look forward to your com-

ments. It is, without question, a balanced roster of experts in this field, so we are really blessed to have you here.

Last Congress, we held significant hearings that jump-started the discussion on the state of online protection as well as the legal basis underpinning the modern internet ecosystem, as you have heard today, and of course the future of content moderation as algorithms now determine much of what we see online. That is an issue our constituents want to know more about.

Today we will undertake a deeper review of Section 230 of the Communications Decency Act portion of the 1996 Telecommunications Act.

In August of this year, as you just heard, Chairman Pallone and I raised the issue of the appearance of export language mirroring Section 230 in trade agreements. We did that in a letter to the U.S. Trade Representative, Robert Lighthizer. We expressed concerns of this internet policy being taken out of the context of its intent and that in the future, the Office of the United States Trade Representative should consult our committee in advance of negotiating on these very issues.

Unfortunately, we have learned that derivative language of Section 230 appeared in an agreement with Japan and continues to be advanced in other discussions. We are very frustrated about that, and I hope the administration is paying attention and listening because they haven't up to this point on this matter.

The USTR does not appear to be reflecting the scrutiny the administration itself says they are applying to how CDA 230 is being utilized in American society. That makes it even more alarming for the USTR to be exporting such policies without the involvement of this committee.

To be clear, this section of the 1996 Telecom Act served as the foundation for the Information Age. So we are here by no means to condemn but rather to understand what truly is and see that the entirety of this section is faithfully followed rather than cherry-picking just a portion.

I want to go back to the trade piece. You know, I thought the letter to the Ambassador was going to send the right message. We are not trying to blow up USTR or USMCA. I voted for every trade agreement going forward. I am a big free trader. But we are getting blown off on this, and I am tired of it. So let it be clear.

Then we found out it is in the Japan agreement. So, you know, clearly they are not listening to our committee or us. So we are serious about this matter. We have not heard from USTR, and this is a real problem. So take note.

If we only refer to Section 230 as "the 26 words that created the internet," as has been popularized by some, we are already missing the mark since, by our word count, which you can use software to figure out, that excludes the Good Samaritan obligations in Section (c)(2). So we should start talking more about that section as the 83 words that can preserve the internet.

All the sections and provisions of CDA 230 should be clearly taken together and not apart. Many of our concerns can be readily addressed if companies just enforce their terms of service.

To put that in better context, I believe a quick history lesson is in order. Today's internet looks a lot different than the days that

CompuServe and Prodigy and the message boards dominated the internet in the 1990s. While the internet is more dynamic and content rich than ever before, there were problems in its infancy managing the vast amounts of speech occurring online.

As our friend Chris Cox, former Member, the author of the legislation, alum of this committee, pointed out on the House floor during debate over his amendment, “No matter how big the army of bureaucrats, it is not going to protect my kids because I do not think the Federal Government will get there in time.” That is his quote.

So Congress recognized then, as we should now, that we need companies to step up to the plate and curb harmful and illegal content from their platforms. The internet is not something to be regulated and managed by government.

Upon enactment, CDA 230 clearly bestowed on providers and users the ability to go after the illegal and harmful content without fear of being held liable in court.

Now, while the law was intended to empower, we have seen social media platforms slow to clean up sites while being quick to use immunity from legal responsibility for such content. In some cases, internet platforms have clearly shirked the responsibility for the content on their platform.

The broad liability shield now in place through common law has obscured the central bargain that was struck, and that is the internet platforms with user-generated content are protected from liability in exchange for the ability to make good faith efforts to moderate harmful and illegal content.

So let me repeat for those that want to be included in the “interactive computer services” definition: Enforce your own terms of service.

I look forward to an informative discussion today on differentiating constitutionally protected speech from illegal content, how we should think of CDA 230 protections for small entities versus large ones, and how various elements of the internet ecosystem shape what consumers see or don’t see.

With that, Mr. Chairman, thank you for having this hearing, and I look forward to getting all the feedback from the witnesses, but, indeed, I have to go up to the other hearing. So thank you very much.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Thank you, Mr. Chairman. I want to welcome our witnesses to this hearing—it is without question a balanced roster of experts in the field. Last Congress, we held significant hearings that jump-started the discussion on the state of online protections, as well as the legal basis underpinning the modern internet ecosystem, and of course the future of content moderation as algorithms now determine much of what we see online. Today, we will undertake a deeper review of Section 230 of the Communications Decency Act portion of the 1996 Telecommunications Act.

In August of this year, Chairman Pallone and I raised the issue of the appearance of export of language mirroring Section 230 in trade agreements in a letter to United States Trade Representative Robert Lighthizer. We expressed concerns of this internet policy being taken out of the context of its intent, and that in the future the Office of the United States Trade Representative should consult our committee in advance of negotiating on these issues. Unfortunately, we have learned that derivative language of Section 230 appeared in an agreement with Japan and

continues to be advanced in other discussions. The USTR does not appear to be reflecting the scrutiny the administration itself is applying to how CDA 230 is being utilized in American society, making it even more alarming for the USTR to be exporting such policies without the involvement of this committee.

To be clear, this section of the '96 Telecom Act served as a foundation for the Information Age, so we are here by no means to condemn, but rather to understand what it truly is, and see that the entirety of the section is faithfully followed rather than cherry-picking just a portion. If we only refer to Section 230 as “the 26 words that created the internet,” as has been popularized by some, we are already missing the mark since, by my word count, that excludes the Good Samaritan obligations in section “c2.” We should start talking more about that section as the 83 words that can preserve the internet. All of the provisions of CDA 230 should be clearly taken together and not apart, and many of our concerns can be readily addressed if companies just enforce their terms of service. To put that in better context, I believe a quick history lesson is in order.

Today’s internet looks a lot different than when CompuServe, Prodigy, and the message boards dominated the internet in '90s. While the internet is more dynamic and content-rich today than ever before, there were problems in its infancy managing the vast amount of speech occurring online. As our friend Chris Cox, the author of the legislation and an alum of this committee, pointed out on the House floor during debate over his amendment, “No matter how big the army of bureaucrats, it is not going to protect my kids because I do not think the Federal Government will get there in time.” So, Congress recognized then, as we should now, that we need companies to step up to the plate and curb harmful and illegal content from their platforms—the internet is not something to be regulated and managed by a government.

Upon enactment, CDA 230 clearly bestowed on providers and users the ability to go after the illegal and harmful content without fear of being held liable in court. While the law was intended to empower, we have seen social media platforms slow to clean up sites while being quick to use immunity from legal responsibility for such content. In some cases, internet platforms have clearly shirked responsibility for the content on their platform.

The broad liability shield now in place through common law has obscured the central bargain that was struck: internet platforms with user-generated content are protected from liability in exchange for the ability to make good faith efforts to moderate harmful and illegal content.

So, let me repeat for those that want to be included in the “interactive computer services” definition: enforce your own terms of service.

I look forward to an informative discussion today on differentiating constitutionally protected speech from illegal content; how we should think of CDA 230 protections for small entities versus large ones; and how various elements of the internet ecosystem shape what consumers see or don’t see.

Again, I hope today’s discussion will help us back on the road to a balance for the betterment of our society. Thank you again to our witnesses for sharing their time and expertise.

Mr. DOYLE. So the administration doesn’t listen to you guys either, huh?

Mr. WALDEN. My statement spoke for itself pretty clearly, I think. We will find out if they are listening or not.

Mr. DOYLE. The gentleman yields back.

I will reiterate that, pursuant to the committee rules, all Members’ written opening statements will be made part of the record.

We now want to introduce our witnesses for today’s hearing.

Mr. Steve Huffman, cofounder and CEO of Reddit.

Welcome.

Ms. Danielle Keats Citron, professor of law at Boston University School of Law.

Welcome.

Dr. Corynne McSherry, legal director of the Electronic Frontier Foundation.

Welcome.

Ms. Gretchen Peters, executive director of the Alliance to Counter Crime Online.

Welcome.

Ms. Katherine Oyama, global head of intellectual property policy for Google.

Welcome.

And Dr. Hany Farid, professor at the University of California, Berkeley.

Welcome to all of you. We want to thank you for joining us today. We look forward to your testimony.

At this time, the Chair will recognize each witness for 5 minutes to provide their opening statement.

Before we begin, I would like to explain our lighting system. In front of you is a series of lights. The light will initially be green at the start of your opening statement. The light will turn yellow when you have 1 minute remaining. Please wrap up your testimony at that point. When the light turns red, we just cut your microphone off. No, we don't, but try to finish before then.

So, Mr. Huffman, we are going to start with you, and you are recognized for 5 minutes.

STATEMENTS OF STEVE HUFFMAN, COFOUNDER AND CHIEF EXECUTIVE OFFICER, REDDIT, INC.; DANIELLE KEATS CITRON, PROFESSOR OF LAW, BOSTON UNIVERSITY SCHOOL OF LAW; CORYNNE MCSHERRY, PH.D., LEGAL DIRECTOR, ELECTRONIC FRONTIER FOUNDATION; GRETCHEN PETERS, EXECUTIVE DIRECTOR, ALLIANCE TO COUNTER CRIME ONLINE; KATHERINE OYAMA, GLOBAL HEAD OF ECONOMIC PROPERTY POLICY, GOOGLE; AND HANY FARID, PH.D., PROFESSOR, UNIVERSITY OF CALIFORNIA, BERKELEY

STATEMENT OF STEVE HUFFMAN

Mr. HUFFMAN. Thank you. Good morning, chairpersons, ranking members, members of the committee. Thank you for inviting me. My name is Steve Huffman. I am the cofounder and CEO of Reddit, and I am grateful for this opportunity to share why 230 is critical to our company and the open internet.

Reddit moderates content in a fundamentally different way than other platforms. We empower communities, and this approach relies on 230. Changes to 230 pose an existential threat not just to us but to thousands of startups across the country, and it would destroy what little competition remains in our industry.

My college roommate and I started Reddit in 2005 as a simple user-powered forum to find news and interesting content. Since then, it has grown into a vast community-driven site where millions of people find not just news and a few laughs but new perspectives and a real sense of belonging. Reddit is communities, communities that are both created and moderated by our users.

Our model has taken years to develop, with many hard lessons learned along the way. As some of you know, I left the company in 2009, and for a time Reddit lurched from crisis to crisis over questions of moderation that we are discussing today.

In 2015, I came back because I realized the vast majority of our communities were providing an invaluable experience for our users and Reddit needed a better approach to moderation.

The way Reddit handles content moderation today is unique in the industry. We use a governance model akin to our own democracy, where everyone follows a set of rules, has the ability to vote and self-organize, and ultimately shares some responsibility for how the platform works.

First, we have our content policy, the fundamental rules that everyone on Reddit must follow. Think of these as our Federal laws. We employ a group, including engineers and data scientists, collectively known as the “Anti-Evil” Team, to enforce these policies.

Below that, each community creates their own rules, State laws, if you will. These rules, written by our volunteer moderators themselves, are tailored to the unique needs of their communities and tend to be far more specific and complex than ours.

The self-moderation our users do every day is the most scalable solution to the challenges of moderating content online.

Individual users play a crucial role as well. They can vote up or down on any piece of content, posts or comments, and report it to our Anti-Evil Team. Through this system of voting and reporting, users can accept or reject any piece of content, thus turning every user into a moderator.

The system isn’t perfect. It is possible to find things on Reddit that break the rules. But its effectiveness has improved with our efforts. Independent academic analysis has shown our approach to be largely effective in curbing bad behavior.

And when we investigated Russian attempts at manipulating our platform in 2016, we found that, of all accounts that tried, less than 1 percent made it past the routine defenses of our team, community moderation, and simple down votes from everyday users.

We also constantly evolve our content policies, and since my return we have made a series of updates addressing violent content, deepfaked pornography, controlled goods, and harassment.

These are just a few of the ways we have worked to moderate in good faith, which brings us to the question of what Reddit would look like without 230.

For starters, we would be forced to defend against anyone with enough money to bankroll a lawsuit, no matter how frivolous. It is worth noting that the cases most commonly dismissed under 230 are regarding defamation. As an open platform where people are allowed to voice critical opinions, we would be a prime target for these, effectively enabling censorship through litigation.

Even targeted limits to 230 will create a regulatory burden on the entire industry, benefiting the largest companies by placing a significant cost on smaller competitors.

While we have 500 employees and a large user base, normally more than enough to be considered a large company, in tech today we are an underdog compared to our nearest competitors, who are public companies 10 to 100 times our size. Still, we recognize that there is truly harmful material on the internet, and we are committed to fighting it.

It is important to understand that rather than helping, even narrow changes to 230 can undermine the power of community and

hurt the vulnerable. Take the opioid epidemic, which has been raised in discussions on 230. We have many communities on Reddit where users struggling with addiction can find support to help them on their way to sobriety.

Were there a carveout in this area, posting them may simply become too risky, forcing us to close them down. This would be a disservice to people who are struggling, yet this is exactly the type of decision that restrictions on 230 would force on us.

Section 230 is a uniquely American law with a balanced approach that has allowed the internet and platforms like ours to flourish while also incentivizing good faith attempts to mitigate the unavoidable downsides of free expression. While these downsides are serious and demand the attention of both us and industry and you in Congress, they do not outweigh the overwhelming good that 230 has enabled.

Thank you. I look forward to your questions.
[The prepared statement of Mr. Huffman follows:]

**U.S. House of Representatives Committee on Energy and Commerce:
Subcommittees on Communications & Technology and Consumer Protection & Commerce
Hearing on “Fostering a Healthier Internet to Protect Consumers”**

**Testimony Submitted for the Record by
Mr. Steve Huffman, Co-Founder & CEO of Reddit, Inc.**

October 16, 2019

I. Introduction

Chairpersons, Ranking Members, Members of the Committee:

Thank you for inviting me. My name is Steve Huffman. I am the co-founder and CEO of Reddit, and I’m grateful for this opportunity to share why Section 230 is critical to our company. Reddit uses a different model of content moderation from our peers—one that empowers communities—and this model relies on Section 230. I’m here because even small changes to the law will have outsized consequences for our business, our communities, and what little competition remains in our industry.

II. What Reddit is and how we approach content moderation

My college roommate and I started Reddit in 2005 as a simple, user-powered forum to find news and interesting content. Since then, it’s grown into a vast, community-driven site, where millions of people find not just news and a few laughs, but also support, new perspectives, and a real sense of belonging.

We don’t think of Reddit as social media, because social media revolves around individuals, while we’re organized around communities. These communities, which are centered upon everything from history and science to advice on relationships and parenting, are both created and moderated by users.

Our model has taken years to develop, with many hard lessons along the way. As some of you know, I left the company in 2009, and for a time Reddit lurched from crisis to crisis over the questions of moderation we’re discussing today. In 2015, I came back because I realized the vast majority of our communities were providing an invaluable experience to our users, and Reddit needed a better approach to moderation.

A. Approach to Moderation

The way Reddit handles content moderation today is unique in the industry. We use a governance model akin to our own democracy—where everyone follows a set of rules, has the ability to vote and self-organize, and ultimately shares some responsibility for how the platform works.

B. Content Policy

First, we have our Content Policy,¹ the fundamental rules everyone on Reddit must follow. We set them ourselves at the corporate level. Think of these as our federal laws. They are principles-based and include things most everyone can agree on, such as prohibitions on harassment, sharing sexual images without consent, encouraging violence, sharing people’s private information, and other behaviors that have no place on our site.

C. Community Rules & Volunteer Moderators

Next, we have rules for what’s allowed in each community—our state laws, if you will. These are written and enforced not by Reddit employees, but by the community’s own volunteer moderators. These rules

¹ <https://www.redditinc.com/policies/content-policy>

are tailored to the unique needs of its members, and tend to be far more specific than the “federal” rules we set. For example, one community devoted to open dialogue between users with different perspectives has a set of rules roughly the length of the US Constitution. Volunteer community moderators are empowered to remove any post that does not follow the community rules, without any involvement or direction from Reddit, Inc. The self-moderation our users do every day at this community level is the most scalable solution we’ve seen to the challenges of moderating content online.

D. Upvotes & Downvotes

Each individual user plays a crucial role as well, voting up or down on every post and comment. Through this system of voting, users can accept or reject any piece of content. While most platforms have some version of the upvote function, an action to convey approval or agreement, we at Reddit see the additional downvote as equally important. The downvote is where community culture is made, through rejecting transgressive behavior or low-quality content. If any community member, not just a moderator, sees poor quality content, they may downvote it, and as people do so, it becomes less visible, and in the case of a comment, disappears from the default view of the community. Thus, Reddit’s voting system essentially turns every user into a content moderator.

Additionally, accrued upvotes and downvotes feed into the posting user’s reputation score, which we call “karma,” which is publicly visible to all other users. It’s an indicator of the constructiveness of a user’s participation on Reddit, and it’s possible for karma to be negative. Quantifying a user’s reputation in this way incentivizes good behavior.

E. Moderation actions taken by Reddit, Inc.

While this user-led system generally works well, we recognize that we as a company still have responsibilities, and we proactively work to ensure communities stay within our rules. Any user may report violations directly to a specialized group of employees at Reddit known as our “Anti-Evil” Team. Their role is to enforce the rules against malicious users, or take down particularly egregious content violations. We can take action against individual users (for example, through account suspensions), or against entire communities. We try to be as transparent as possible when we take such actions, and we publish our content policy enforcement actions annually in our Transparency Report. Our decisions are also appealable, and we likewise publish the appeal intake and acceptance rate in the Transparency Report.² Owing to these practices, we are proud that we were the only company to earn a perfect six-star rating from the Electronic Frontier Foundation in their annual “Who Has Your Back?” report on tech company transparency.³

We also evolve our policies to ensure they keep up with reality. Since my return we’ve made a series of updates addressing violent content, deepfaked pornography, controlled goods, and harassment.

Nevertheless, like our democracy, the system isn’t perfect, though its effectiveness has improved with our efforts. An independent scholarly analysis of our 2015 banning of communities that didn’t abide by our policies showed these actions were largely effective in curbing bad behavior.⁴ And when we investigated Russian attempts at manipulating our platform in 2016, we found that, of all accounts that tried, less than 1% made it past the routine defenses of our content policy, community moderation, and simple downvotes from everyday users.⁵

² <https://www.redditinc.com/policies/transparency-report-2018>

³ <https://www.eff.org/wp/who-has-your-back-2019>

⁴ <http://comp.social.gatech.edu/papers/cscw18-chand-hate.pdf>

⁵ https://www.reddit.com/r/announcements/comments/8bb85p/reddits_2017_transparency_report_and_suspect/

While our model has improved the past few years, there is and will always be more to do and ways for us to improve, particularly as our communities grow and raise new and more complicated issues for us to solve. Section 230 is an instrumental tool in allowing us to do this work in good faith, without facing liability for it.

III. What does a world without 230 look like?

This all begs the question of what Reddit (and the internet economy at large) would look like without Section 230.

A. We wouldn't be able to moderate

First, all of the improvements in content moderation we've made over the past few years could not have happened, as these good-faith actions would expose us to liability. It's worth noting how much the Reddit of today looks like the Prodigy of the early 90s, which raised the case that delivered 230. Perversely, because Prodigy had moderators who removed egregious content, they were held liable for all content. At the same time, other services, notably CompuServe, who didn't make any attempts at moderating even the very worst content, were safe from legal consequences. This backwards incentive structure might have made sense in a pre-Internet age when publishers were dealing with much smaller amounts of content, but the sheer volume of content generated on internet platforms today means that all-or-nothing moderation simply isn't feasible. For example, on average Reddit handles more than 750,000 posts and 6.3 million comments per day across over 130,000 active communities.

B. Market competition considerations

There are also market considerations for 230 that are especially applicable to a smaller company like Reddit. Even targeted limits to 230 will create a regulatory burden on the entire industry, benefiting the largest companies by placing a significant cost on smaller competitors. While we have 500 employees and a sizable user base—normally more than enough to be considered a large company—in tech today we are an underdog compared to our nearest competitors, who are public companies 10 to 100 times our size.

Many of the conversations on revising 230 are premised on companies having the ability to moderate content from the center, in an industrialized model often reliant on armies of tens of thousands of contractors. Medium, small, and startup-sized companies don't have the resources for this. This approach has questionable utility anyway, since even tens of thousands of contractors don't scale with hundreds of millions of users, let alone billions. Indeed, the only thing that scales with users is users themselves, which is why we've empowered ours the way we have.

But to speak even more fundamentally about competition and startups, I think back to the early days of Reddit. Had we been liable for every piece of content on Reddit, we would have been immediately vulnerable to lawsuits. And statistically speaking, most of those cases would not have been about the serious harms we are all concerned with—illicit drug sales, terrorist propaganda, and other issues—but rather defamation, which is far and away the largest class of suits dismissed on 230 grounds. Indeed, it was a \$200 million defamation lawsuit that saddled Prodigy in the 230 origin story. We and others would be forced to defend against anyone with enough money to bankroll a lawsuit, no matter how frivolous, effectively enabling censorship through litigation.

C. Human considerations

Still, we recognize that there is truly harmful material on the internet, and we are committed to fighting it. But it's important to understand that rather than helping, even narrow changes to 230 can undermine the power of community, chill discussion, and hurt the vulnerable.

Take the opioid epidemic, which has been raised in discussions about 230. We have many communities on Reddit where users struggling with addiction can find support to help them on their way to sobriety.

Were there to be a carve-out in this area, hosting them may simply become too risky, forcing us to close them down. This would be a disservice to people who are struggling, yet this is exactly the type of decision that restrictions to 230 would force on us.

IV. Conclusion

Section 230 is a uniquely American law with a balanced approach that has allowed the internet and platforms like ours to flourish, while incentivizing good faith attempts to mitigate the unavoidable downsides of free expression. While these downsides are serious and demand the attention of both us in industry and you in Congress, they do not outweigh the overwhelming good that 230 has enabled.

Thank you, and I look forward to your questions.

Mr. DOYLE. Thank you, Mr. Huffman.
 Ms. Citron, you are recognized for 5 minutes.

STATEMENT OF DANIELLE KEATS CITRON

Ms. CITRON. Thank you for having me and for having such a thoughtful bench with me on the panel.

When Congress adopted Section 230 twenty years ago, the goal was to incentivize tech companies to moderate content. And although Congress, of course, wanted the internet, what they could imagine it at that time, to be open and free, they also knew that openness would risk offensive material, and I am going to use their words. And so what they did was devise an incentive, a legal shield for Good Samaritans who are trying to clean up the internet, both accounting for the failure to remove, so underfiltering, and overfiltering of content.

Now, the purpose of the statute was fairly clear, but its interpretation, the words weren't, and so what we have seen are courts massively overextending Section 230 to sites that are irresponsible in the extreme and that produce extraordinary harm. Now, we have seen the liability shield be applied to sites whose entire business model is abuse. So revenge porn operators and sites that all they do is curate users' deepfake sex videos, they get to enjoy immunity, and have, from liability.

And interestingly, not only is it bad Samaritans who have enjoyed the legal shield from responsibility, but it is also sites that really have nothing to do with speech, that traffic in dangerous goods, like Armslist.com. And the costs are significant. This overbroad interpretation allows bad Samaritan sites, reckless, irresponsible sites, to really have costs on people's lives.

I am going to take the case of online harassment because I have been studying it for the past 10 years. The costs are significant, and especially to women and minorities. Online harassment that is often hosted on these sites is costly to people's central life opportunities.

So when a Google search of your name contains rape threats, your nude photo without your consent, your home address because you have been doxxed, and lies and defamation about you, it is hard to get a job and it is hard to keep a job. And also for victims, they are driven offline in the face of online assaults. They are terrorized. They often change their names, and they move.

And so in many respects, the calculus, the free speech calculus, it is not necessarily a win for free speech, as we are seeing really diverse viewpoints and diverse individuals being chased offline.

So now the market, I think, ultimately is not going to solve this problem. So many of these businesses, they make money off of online advertising and salacious, negative, and novel content that attracts eyeballs. So the market itself I don't think we can rely on to solve this problem.

So, of course, legal reform. The question is, how should we do it?

I think we have to keep Section 230. It has tremendous upsides. But we should return it to its original purpose, which was to condition the shield on being a Good Samaritan, on engaging in what Ben Wittes and I have called reasonable content moderation practices.

Now, there are other ways to do it. In my testimony, I sort of draw up some solutions. But we have got to do something because doing nothing has cost. It says to victims of online abuse that their speech and their equality is less important than the business profits of some of these most harmful platforms.

Thank you.

[The prepared statement of Ms. Citron follows:]

PREPARED WRITTEN TESTIMONY AND STATEMENT FOR THE RECORD FOR

Danielle Keats Citron,
Professor of Law, Boston University School of Law

HEARING ON

“Fostering a Healthier Internet to Protect Consumers”

BEFORE THE

House Committee on Energy and Commerce

October 16, 2019

John D. Dingell Room, 2123, Rayburn House Office Building

Washington, D.C.

INTRODUCTION

Thank you for inviting me to appear before you to testify about corporate responsibility for online activity and fostering a healthy internet to protect consumers. My name is Danielle Keats Citron. I am a Professor of Law at the Boston University School of Law. In addition to my home institution, I am an Affiliate Faculty at the Berkman Klein Center at Harvard Law School, Affiliate Scholar at Stanford Law School's Center on Internet & Society, Affiliate Fellow at Yale Law School's Information Society Project, and Tech Fellow at NYU Law's Policing Project. I am also a 2019 MacArthur Fellow.

My scholarship focuses on privacy, free speech, and civil rights. I have published more than 30 articles in major law reviews and more than 25 opinion pieces for major news outlets.¹ My book *Hate Crimes in Cyberspace* tackled the phenomenon of cyber stalking and what law, companies, and society can do about it.² As a member of the American Law Institute, I serve as an adviser on *Restatement (Third) Torts: Defamation and Privacy* and the *Restatement (Third) Information Privacy Principles Project*. In my own writing and with coauthors Benjamin Wittes, Robert Chesney, Quinta Jurecic, and Mary Anne Franks, I have explored the significance of Section 230 to civil rights and civil liberties in a digital age.³

* * *

Summary: In the early days of the commercial internet, lawmakers recognized that federal agencies could not possibly tackle all noxious activity online. Tech companies, in their view, were essential partners to that task. An early judicial decision, however, imperiled that possibility by

¹ See, e.g., Danielle Keats Citron, *Why Sexual Privacy Matters for Trust*, 96 WASH. U. L. REV. (forthcoming 2019); *Sexual Privacy*, 128 YALE L.J. 1870 (2019); *When Law Frees Us to Speak*, 87 FORDHAM L. REV. 2317 (2019) (with Jonathon Penney); *Four Principles for Digital Speech*, 95 WASH. U. L. REV. 1353 (2018) (with Neil Richards); *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035 (2018); *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEXAS L. REV. (2018) (with Daniel J. Solove); *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016); *Spying Inc.*, 72 WASH. & LEE L. REV. 1243 (2015); *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014) (with Mary Anne Franks); *The Scored Society*, 89 WASH. L. REV. 1 (2014) (with Frank Pasquale); *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013) (with David Gray); *Intermediaries and Hate Speech: Fostering Digital Citizenship for the Information Age*, 91 B.U. L. REV. 1435 (2011) (with Helen Norton); *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441 (2011) (with Frank Pasquale); *Mainstreaming Privacy Torts*, 99 CAL. L. REV. 1805 (2010); *Government Speech 2.0*, 87 DENVER U. L. REV. 899 (2010) (with Helen Norton); *Fulfilling Government 2.0's Promise with Robust Privacy Protections*, 78 GEO. WASH. L. REV. 822 (2010); *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373 (2009); *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009); *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008); *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007).

² DANIELLE KEATS CITRON, *HATE CRIMES IN CYBERSPACE* (2014).

³ See, e.g., Danielle Keats Citron, *Cyber Mobs, Disinformation, and Death Videos: The Internet As It Is (and as It Should Be)*, MICH. L. REV. (forthcoming 2020) (reviewing NICK DRNASO, SABRINA (2018)); *The Internet as a Speech-Conversion Machine and Other Myths Confounding Tech Policy Reform*, U. CHI. LEGAL FORUM (forthcoming 2020) (with Mary Anne Franks); *Deep Fakes: The Looming Crisis for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. (forthcoming 2019) (with Robert Chesney); *Section 230's Challenge to Civil Rights and Civil Liberties*, KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY (Apr. 6, 2008), <https://knightcolumbia.org/content/section-230s-challenge-civil-rights-and-civil-liberties>; *Platform Justice: Content Moderation at an Inflection Point*, HOOVER INST. (2018) (with Quinta Jurecic); *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 FORDHAM L. REV. 401 (2017) (with Benjamin Wittes); *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009).

ruling that platforms' content-moderation efforts increased the risk of liability.⁴ Lawmakers were appalled that online services would be penalized for self-regulation. Section 230 of the Communications Decency Act was a direct repudiation of that ruling. Congress wanted to incentivize private efforts to filter, block, or otherwise address troubling online activity.⁵ Section 230 provided that incentive by securing a shield from legal liability for under- or over-filtering "offensive" content.⁶

Section 230 has helped secure opportunities to work, speak, and engage online. But it has not been a clear win for civil rights and civil liberties. Its overbroad interpretation in the courts has undermined the statute's purpose and exacted significant costs to free speech and equal opportunity. Platforms not only have been shielded from liability when their moderation efforts have filtered or blocked too much or too little "offensive" or illegal activity, as lawmakers intended. But they also have been shielded from responsibility even then they solicit illegal activities, deliberately leave up unambiguously illegal content that causes harm, and sell dangerous products. The costs to free expression and equality have been considerable, especially for women, nonwhites, and LGBTQ individuals. Section 230 should be revised to condition the legal shield on reasonable content moderation practices in the face of clear illegality that causes demonstrable harm. That would return the statute to its original purpose—to allow companies to act more responsibly, not less.

* * *

I. *Section 230's History and Purpose*

The Communications Decency Act (CDA), part of the Telecommunications Act of 1996, was introduced to make the internet safer for kids and to address concerns about pornography. Besides proposing criminal penalties for the distribution of sexually explicit material online, members of Congress underscored the need for private sector help in reducing the volume of "offensive" material online. Then-Representatives Christopher Cox and Ron Wyden offered an amendment to the CDA entitled "Protection for Private Blocking and Screening of Offensive Material."⁷ The Cox-Wyden Amendment, codified as Section 230, provided immunity from liability for "Good Samaritan" online service providers that over- or under-filtered objectionable content.⁸

Section 230(c), entitled "Good Samaritan blocking and filtering of offensive content," has two key provisions. Section 230(c)(1) specifies that providers or users of interactive computer services will not be treated as publishers or speakers of user-generated content.⁹ Section 230(c)(2) says that online service providers will not be held liable for good-faith filtering or blocking of user-

⁴ See *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). For a superb history of Section 230 and the cases leading to its passage, see JEFF KOSSEFF, *THE TWENTY-SIX WORDS THAT CREATED THE INTERNET* (2019).

⁵ CITRON, *HATE CRIMES IN CYBERSPACE*, *supra* note, at 170-73.

⁶ Citron & Wittes, *supra* note, at 404-06.

⁷ *Id.*

⁸ *Id.*

⁹ 47 U.S.C. § 230(c)(1).

generated content.¹⁰ Section 230 carves out exceptions from its immunity provisions, including federal criminal law, intellectual property law, and the Electronic Privacy Communications Act.¹¹

In 1996, lawmakers could hardly have imagined the role that the internet would play in modern life. Yet Section 230's authors were prescient. In their view, "if this amazing new thing – the Internet – [was] going to blossom," companies should not be "punished for *trying* to keep things clean."¹² Cox recently explained that, "the original purpose of [Section 230] was to help clean up the Internet, not to facilitate people doing bad things on the Internet."¹³ The key to Section 230, Wyden agreed, was "making sure that companies in return for that protection – that they wouldn't be sued indiscriminately – were being responsible in terms of policing their platforms."¹⁴

II. *Overbroad Judicial Interpretation*

The judiciary's interpretation of Section 230 has not squared with this vision. Rather than an immunity for responsible moderation efforts, courts have stretched Section 230's legal shield far beyond what its words, context, and purpose support.¹⁵ Section 230 has been read to immunize platforms from liability even though they knew about users' illegal activity, deliberately refused to remove it, and ensured that those responsible for the illegality could not be identified.¹⁶ It has provided a legal shield from liability to platforms that solicited users to engage in tortious and illegal activity.¹⁷ It has been read to absolve platforms of liability even though they designed their sites to enhance the visibility of illegal activity and to ensure that the perpetrators could not be identified and caught.¹⁸

Courts have attributed this broad-sweeping approach to the fact that "First Amendment values [drove] the CDA."¹⁹ For support, court have pointed to Section 230's "findings" and "policy" sections, which highlight the importance of the "vibrant and competitive free market that presently exists" for the internet and the internet's role in facilitating "myriad avenues for intellectual activity" and the "diversity of political discourse."²⁰ As Mary Anne Franks has underscored, Congress' stated goals also included the:

development of technologies that "maximize user control over what information is received" by Internet users, as well as the "vigorous enforcement of Federal criminal laws to deter and publish trafficking in obscenity, stalking and harassment by means of the computer." In other

¹⁰ 47 U.S.C. § 230(c)(2).

¹¹ 47 U.S.C. § 230(e).

¹² See Citron & Jurecic, *supra* note.

¹³ *Id.*

¹⁴ *Id.*

¹⁵ Citron & Wittes, *supra* note, at 406-10.

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ Citron, *Section 230's Challenge to Civil Rights and Civil Liberties*, *supra* note. See generally Olivier Sylvain, *Intermediary Design Duties*, 50 CONN. L. REV. 1 (2017).

¹⁹ Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 18 (1st Cir. 2016), cert. denied, 137 S. Ct. 622 (2017).

²⁰ See, e.g., Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009).

words, the law [wa]s intended to promote the values of privacy, security and liberty alongside the values of open discourse.²¹

Section 230's liability shield has been extended to shield activity that has little to do with free speech, including the sale of dangerous products.²² Consider Armslist.com, the self-described "firearms marketplace."²³ Unlicensed sellers use the site to sell guns to people who cannot pass background checks.²⁴ Armslist.com is where Radcliffe Haughton illegally purchased a gun, which he used to murder his estranged wife who had a restraining order against him.²⁵ The Wisconsin court's restraining order banned Haughton from legally purchasing a firearm.²⁶ On Armslist.com, Haughton found a gun seller that did not require a background check.²⁷ He used the gun that he illegally purchased to murder his estranged wife and two co-workers.²⁸ The Wisconsin Supreme Court held that Armslist was immune from liability based on Section 230.²⁹

Extending the immunity from liability to platforms that deliberately encourage, facilitate, or refuse to remove illegal activity would seem absurd to the CDA's drafters. But even more absurd is immunizing from liability enterprises that connect sellers of deadly weapons with prohibited buyers for a cut of the profits. Armslist.com can hardly be said to "provide 'educational and informational resources' or contribute to 'the diversity of political discourse.'"³⁰

III. *Evaluating the Status Quo*

Section 230's overbroad interpretation means that platforms have little legal incentive to combat online abuse. Rebecca Tushnet put it well a decade ago: Section 230 ensures that platforms enjoy "power without responsibility."³¹ Market forces are unlikely to encourage responsible content moderation. Platforms make their money through online advertising generated when users like, click, and share.³² Thus, allowing attention-grabbing abuse to remain online accords with platforms' rational self-interest. Platforms "produce nothing and sell nothing except advertisements and information about users, and conflict among those users may be good for business."³³ If a company's analytics suggest that people pay more attention to content that makes

²¹ Mary Anne Franks, *The Lawless Internet? Myths and Misconceptions About CDA Section 230*, HUFFINGTON POST (Feb. 17, 2014).

²² See, e.g., *Hinton v. Amazon.com, LLC*, 72 F. Supp. 3d 685, 687, 690 (S.D. Miss. 2014).

²³ <https://www.armslist.com/>

²⁴ See Mary Anne Franks, *Our Collective Responsibility for Mass Shootings*, N.Y. TIMES, October 11, 2019, available at <https://www.nytimes.com/2019/10/09/opinion/mass-shooting-responsibility.html>.

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

²⁸ *Id.*

²⁹ *Id.* The non-profit organization the Cyber Civil Rights Initiative, of which I am the Vice President alongside Dr. Mary Anne Franks who serves as its President, has filed an amicus brief in support of the petitioner's request for writ of certiorari in the Supreme Court. Brief of Amicus Curiae of Cyber Civil Rights Initiative and Legal Academics in Support of Petitioners in *Yasmine Daniel v. Armslist.com*, available at https://www.supremecourt.gov/DocketPDF/19/19-153/114340/20190830155050530_Brief.PDF

³⁰ Amicus Curiae of Cyber Civil Right Initiative, *supra* note 29, at 16.

³¹ Rebecca Tushnet, *Power without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986 (2008).

³² Mary Anne Franks, *Justice Beyond Dispute*, 131 HARV. L. REV. 1374, 1386 (2018) (reviewing ETHAN KATSH & ORNA RABINOVICH-EINY, *DIGITAL JUSTICE: TECHNOLOGY AND THE INTERNET OF DISPUTES* (2017)).

³³ *Id.*

them sad or angry, then the company will highlight such content.³⁴ Research shows that people are more attracted to negative and novel information.³⁵ Hence, keeping up destructive content may make the most sense for a company's bottom line.

As Federal Trade Commissioner Rohit Chopra powerfully warned in his dissent from the agency's 2019 settlement with Facebook, the behavioral advertising business model is the "root cause of [social media companies'] widespread and systemic problems."³⁶ Online behavioral advertising generates profits by "turning users into products, their activity into assets," and their platforms into "weapons of mass manipulation."³⁷ Tech companies "have few incentives to stop [online abuse], and in some cases are incentivized to ignore or aggravate [it]."³⁸

To be sure, the dominant tech companies do moderate certain content by shadow banning, filtering, or blocking it.³⁹ They have acceded to pressure from the European Commission to remove hate speech and terrorist activity.⁴⁰ They have banned certain forms of online abuse, such as nonconsensual pornography and threats, in response to pressure from users, advocacy groups, and advertisers.⁴¹ Platforms have expended resources to stem abuse when it is a net negative for their bottom line.⁴²

Yet, as we have seen, market pressures do not always point in that direction. The business model of some sites is abuse because such abuse generates online traffic, clicks, and shares.⁴³ Deepfake pornography sites⁴⁴ as well as countless revenge porn sites and gossip sites⁴⁵ thrive thanks to online advertising.

Without question, Section 230 has been valuable to innovation and expression. It has enabled vast and sundry businesses. It has led to the rise of social media companies like Facebook, Twitter, and Reddit. But it also has subsidized platforms that encourage online abuse. It has left victims without leverage to insist that platforms take down destructive activity.

³⁴ Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.*, Commission File No. 1823109, at 2 (July 24, 2019).

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.*

³⁸ Franks, *Justice Beyond Dispute*, *supra* note, at 1386.

³⁹ Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, *supra* note, at 1038-39; Citron & Norton, *Intermediaries and Hate Speech*, *supra* note, at 1468-71.

⁴⁰ Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, *supra* note, at 1038-39.

⁴¹ *Id.* at 1037.

⁴² CITRON, *HATE CRIMES IN CYBERSPACE*, *supra* note, at 229 (discussing how Facebook changed its position on pro rape pages after fifteen companies threatened to pull their ads); Mary Anne Franks, "Revenge Porn" Reform: A View from the Front Lines, 69 FLA. L. REV. 1251 (2017).

⁴³ For instance, eight of the top ten pornography websites host deepfake pornography, and there are nine deepfake pornography websites hosting 13,254 fake porn videos (mostly featuring female celebrities without their consent). These sites generate income from advertising. Indeed, as the first comprehensive study of deepfake video and audio explains, "deepfake pornography represents a growing business opportunity, with all of these websites featuring some form of advertising." Deeptrace Labs, *The State of Deepfakes: Landscape, Threats, and Impact* 6 (September 2019), available at <https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf>.

⁴⁴ *Id.*

⁴⁵ See, e.g., *Erna Besic Psycho Mom of Two!*, THE DIRTY (Oct. 9, 2019, 10:02 AM), <https://thedirty.com/#post-2374229>.

This laissez-faire approach has been costly to individuals, groups, and society. As more than ten years of research have shown, cybermobs and individual harassers target individuals with sexually threatening and sexually humiliating online abuse.⁴⁶ According to a 2017 Pew Research Center study, one in five U.S. adults have experienced online harassment that includes stalking, threats of violence, or cyber sexual harassment.⁴⁷ More often, targeted individuals are women, women of color, lesbian and trans women, and other sexual minorities.⁴⁸ They do not feel safe on- or offline.⁴⁹ They experience anxiety and severe emotional distress. Some victims move and change their names.⁵⁰

In the face of online assaults, victims have difficulty finding employment or keeping their jobs because the abuse appears in searches of their names.⁵¹ Online abuse not only makes it difficult to make a living, but it silences victims.⁵² Targeted individuals often shut down social media profiles, blogs, and accounts.⁵³ As Mary Anne Franks has argued in her important new book *The Cult of the Constitution*, a strike-oriented view of Section 230 has been costly to equal protection.⁵⁴ The benefits Section 230's immunity has enabled likely could have been secured at a lesser price.⁵⁵

IV. Potential Statutory Responses

Reforming Section 230 is long overdue. Before discussing possible options, it is worth noting that efforts are underway to impose Section 230's provisions as part of trade agreement with Mexico and Canada. It is unwise for the Administration to inscribe Section 230 into trade agreements at the same time that efforts are underway in Congress to reform the law.⁵⁶

⁴⁶ See generally CITRON, HATE CRIMES IN CYBERSPACE, *supra* note. The 2017 Pew study found that one in four Black individuals say they have been subject to online harassment due to their race as have one in ten Hispanic individuals. For white individuals, the share is lower—three percent. Women are twice as likely as men to say they have been targeted online due to their gender (11 percent versus 5 percent). Duggan, *supra* note. Other studies have made clear that LGBTQ individuals are particularly vulnerable to online harassment, CITRON, HATE CRIMES IN CYBERSPACE, *supra* note, as well as nonconsensual pornography. Data & Society, Online Harassment, Digital Abuse, and Cyberstalking in America (November 21, 2016), available at https://innovativepublichealth.org/wp-content/uploads/2_Online-Harassment-Report_Final.pdf.

⁴⁷ Maeve Duggan, Online Harassment 2017 Study, Pew Research Center (July 11, 2017).

⁴⁸ CITRON, HATE CRIMES IN CYBERSPACE, *supra* note.

⁴⁹ *Id.*

⁵⁰ Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 125–26 (2016); see also Jonathon W. Penney, *Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study*, 6 INTERNET POL'Y REV., May 26, 2017, at 1, 3. See generally CITRON, HATE CRIMES IN CYBERSPACE, *supra* note, at; Danielle Keats Citron, *Civil Rights In Our Information Age*, in THE OFFENSIVE INTERNET (Saul Levmore & Martha C. Nussbaum, eds. 2010); Citron & Richards, *supra* note, at 1365 (“[N]ot everyone can freely engage online. This is especially true for women, minorities, and political dissenters who are more often the targets of cyber mobs and individual harassers.”); Citron & Franks, *supra* note, at 385; Citron, *Cyber Civil Rights*, *supra* note.

⁵¹ *Id.*

⁵² *Id.*

⁵³ *Id.*

⁵⁴ MARY ANNE FRANKS, THE CULT OF THE CONSTITUTION (2019).

⁵⁵ Citron & Wittes, *supra* note.

⁵⁶ See, e.g., Neil Turkewitz, *NAFTA and Unsafe Harbors: Why Calls for Blanket Immunities Must Be Rejected*, MEDIUM (Jan. 23, 2018). As Rebecca J. Hamilton explores in her important work, there is and should not be a one-size fits all model for online speech regulation given the socio-legal-cultural differences in the global public spheres online. Rebecca J. Hamilton, *Governing the Global Public Sphere* (on file with author).

Some urge Congress to maintain Section 230's immunity but to create an explicit exception from its legal shield for certain types of behavior. A recent example of that approach is the Stop Enabling Sex Traffickers Act (SESTA), which passed by an overwhelming vote in 2016. The bill amended Section 230 by rendering websites liable for knowingly hosting sex trafficking content. That law, however, is flawed. By effectively pinning the legal shield on a platform's lack of knowledge of sex trafficking, the law reprises the dilemma that led Congress to pass Section 230 in the first place. To avoid liability, platforms have resorted to either filtering everything related to sex or sitting on their hands.⁵⁷ That is the opposite of what the drafters of Section 230 wanted.

There are better alternatives. A more effective and modest adjustment would involve amending Section 230 to exclude bad actors from its legal shield. Free speech scholar Geoffrey Stone, for instance, suggests denying the immunity to online service providers that "deliberately leave up unambiguously unlawful content that clearly creates a serious harm to others."⁵⁸

A variant on this theme would deny the legal shield to cases involving platforms that have solicited or induced illegal behavior or unlawful content. This approach takes a page from intermediary liability rules in trademark and copyright law. As Stacey Dogan observed in that context, inducement doctrines allow courts to target bad actors whose business models center on infringement.⁵⁹ Providers that solicit or induce illegality should not enjoy immunity from liability. This approach targets the harmful conduct while providing breathing space for protected expression.⁶⁰

There is a broader, though balanced, legislative fix that Benjamin Wittes and I have proposed. Under our proposal, platforms would enjoy immunity from liability *if* they could show that their content-moderation practices writ large are reasonable. Wittes and I offer a revision to Section 230(c)(1) as follows:

No provider or user of an interactive computer service that *takes reasonable steps to address known unlawful uses of its services that create serious harm to others* shall be treated as the publisher or speaker of any information provided by another information content provider in any action arising out of the publication of content provided by that information content provider.

If adopted, the question before the courts in a motion to dismiss on Section 230 grounds would be whether a defendant employed reasonable content moderation practices in the face of known illegality. The question would not be whether a platform acted reasonably with regard to a specific instance of speech. Instead, the court would ask whether the platform engaged in reasonable content moderation practices writ large with regard to known illegality that creates serious harm to others.⁶¹

⁵⁷ Citron & Jurecic, *supra* note.

⁵⁸ E-mail from Geoffrey Stone, Professor of Law, Univ. of Chi., to author (Apr. 8, 2018).

⁵⁹ Stacey Dogan, *Principled Standards vs. Boundless Discretion: A Tale of Two Approaches to Intermediary Trademark Liability Online*, 37 COLUM. J.L. & ARTS 503, 507-08 (2014).

⁶⁰ *Id.* at 508-09.

⁶¹ Tech companies have signaled their support as well. For instance, IBM issued a statement saying that Congress should adopt our proposal and wrote a tweet to that effect as well. Ryan Hagemann, *A Precision Approach to Stopping Illegal Online Activities*, IBM THINK POLICY (July 10, 2019), <https://www.ibm.com/blogs/policy/cda-230/>; *see also*

The assessment of reasonable content-moderation practices would take into account differences among online entities. Social networks with millions of postings a day cannot plausibly respond to complaints of abuse immediately, let alone within a day or two. On the other hand, they may be able to deploy technologies to detect and filter content that they previously determined was unlawful.⁶² The duty of care will evolve as technology improves.

A reasonable standard of care will reduce opportunities for abuse without interfering with the further development of a vibrant internet or unintentionally turning innocent platforms into involuntary insurers for those injured through their sites. Approaching the problem as one of setting an appropriate standard of care more readily allows differentiating between different kinds of online actors. Websites that solicit illegality or that refuse to address unlawful activity that creates serious harm should not enjoy immunity from liability. On the other hand, social networks that have safety and speech policies that are transparent and reasonably executed at scale should enjoy the immunity from liability as the drafters of Section 230 intended.

To return to Rebecca Tushnet's framing, with power comes responsibility. Law should change to ensure that such power is wielded responsibly. With Section 230, Congress sought to provide incentives for "Good Samaritans" engaged in efforts to moderate content. Their goal was laudable. Section 230 should be amended to condition the immunity on reasonable moderation practices rather than the free pass that exists today. Market pressures and morals are not always enough, and they should not have to be.

BIOGRAPHY

Danielle Citron is a Professor of Law at the Boston University School of Law. She previously taught at the University of Maryland Carey School of Law where she received the 2018 "UMD Champion of Excellence" award for teaching and scholarship. Professor Citron has been a Visiting Professor at Fordham University School of Law (Fall 2018) and George Washington Law School (Spring 2017). Professor Citron teaches and writes about data privacy, free expression, civil rights, and administrative law.

Professor Citron is an internationally recognized privacy expert. She was named a MacArthur Fellow in 2019. Her book *Hate Crimes in Cyberspace* (Harvard University Press) explored the phenomenon of cyber stalking and the role of law and private companies in combating it. The editors of *Cosmopolitan* included her book in its "20 Best Moments for Women in 2014." Professor Citron has published numerous book chapters and more than 30 law review articles, published in the *Yale Law Journal*, *California Law Review*, *Michigan Law Review*, *Harvard Law Review Forum*, *Boston University Law Review*, *Notre Dame Law Review*, *Fordham Law Review*, *George Washington Law Review*, *Minnesota Law Review*, *Texas Law Review*, *Washington University Law Review*, *Southern California Law Review*, *Washington & Lee Law Review*, *Wake Forest Law Review*, *Washington Law*

@RyanLeeHagemann, TWITTER (July 10, 2019, 3:14 PM), <https://twitter.com/RyanLeeHagemann/status/1149035886945939457?s=20> ("A special shoutout to @daniellecitron and @benjaminwittes, who helped to clarify what a moderate, compromise-oriented approach to the #Section230 debate looks like.")

⁶² Citron, *Sexual Privacy*, *supra* note (discussing Facebook's hashing initiative to address nonconsensual distribution of intimate images).

Review, *U.C. Davis Law Review*, *University of Chicago Legal Forum*, and other journals. Her current scholarly projects concern sexual privacy; privacy and national security challenges of deep fakes; and the automated administrative state. Professor Citron's opinion pieces have appeared in major media outlets, including *The New York Times*, *The Atlantic*, *Slate*, *Time*, *CNN*, *The Guardian*, *New Scientist*, *Lawfare*, *ars technica*, and *New York Daily News*. She is a technology contributor for *Forbes* and served as a member of the now-defunct *Concurring Opinions* blog (2008-2019).

Professor Citron's work has been recognized at home and abroad. In 2015, the United Kingdom's *Prospect Magazine* named Professor Citron one of the "Top 50 World Thinkers." *The Maryland Daily Record* named her one of the "Top 50 Most Influential Marylanders." In 2011, Professor Citron testified about misogynistic cyber hate speech before the Inter-Parliamentary Committee on Anti-Semitism at the House of Commons.

Professor Citron is an active member of the cyber law community. She is an Affiliate Scholar at the Stanford Center on Internet and Society, Affiliate Fellow at the Yale Information Society Project, Senior Fellow at Future of Privacy, Affiliate Faculty at the Berkman Klein Center at Harvard Law School, and a Tech Fellow at the NYU Policing Project. She is a member of the American Law Institute (inducted in 2017) and serves as an adviser to the American Law Institute's *Restatement (Third) Information Privacy Principles Project* and *Restatement (Third) Torts: Defamation and Privacy*.

Professor Citron works with civil liberties and privacy organizations. She is the Vice President of the *Cyber Civil Rights Initiative*. She served as the Chair of the *Electronic Privacy Information Center's* Board of Directors from 2017-2019 and now sits on its Board. Professor Citron has served on the Advisory Boards of *Without My Consent*, *Teach Privacy*, and the *International Association of Privacy Professionals* Privacy Bar. In connection with her advocacy work, she advises tech companies on online safety, privacy, and free speech. She serves on Twitter's Trust and Safety Council as well as Facebook's Nonconsensual Intimate Imagery Task Force. She has presented her research at Twitter, Facebook, Google, and Microsoft.

Professor Citron advises federal and state legislators, law enforcement, and international lawmakers on privacy issues. In June 2019, she testified at the House Intelligence Committee hearing on deep fakes and other forms of disinformation. In July 2017, she testified at a congressional briefing on online harassment and sexual violence co-sponsored by Congresswoman Jackie Speier. In April 2015, she testified at a congressional briefing sponsored by Congresswoman Katharine Clark on the First Amendment implications of a federal cyber stalking legal agenda. She has worked with the offices of Congresswoman Jackie Speier, Congresswoman Katharine Clark, Senator Richard Blumenthal, Senator Elizabeth Warren, Senator Kamala Harris, and Senator Diane Feinstein on federal legislation. Professor Citron helped Maryland State Senator Jon Cardin draft a bill criminalizing the nonconsensual publication of nude images, which was passed into law in 2014. From 2014 to December 2016, Professor Citron served as an advisor to then-California Attorney General Kamala Harris. She served as a member of AG Harris's *Task Force to Combat Cyber Exploitation and Violence Against Women*. In October 2015, Professor Citron, with AG Harris, spoke at a press conference to discuss the AG office's new online hub of resources for law enforcement, technology companies, and victims of cyber sexual exploitation.

Professor Citron has presented her research in over 200 talks at federal agencies, meetings of the National Association of Attorneys General, the National Holocaust Museum, the Anti-Defamation League, Wikimedia Foundation, universities, companies, and think tanks. She gave a TED talk on the issue of deep fakes at the 2019 Global TED Summit in Edinburgh, Scotland. She appeared in HBO's *Swiped: Hooking Up in the Digital Age* (directed by Nancy Jo Sales) and *Netizens* (which premiered at the 2018 Tribeca Film Festival, directed by Cynthia Lowen). She has been quoted in hundreds of news stories in publications including *The New York Times*, *Washington Post*, *Wall Street Journal*, *Los Angeles Times*, *San Francisco Chronicle*, *USA Today*, *National Public Radio*, *Time*, *Newsweek*, *the New Yorker*, *New York Magazine*, *Cosmopolitan*, HBO's *Last Week Tonight with John Oliver*, *Barron's*, *Financial Times*, *The Guardian*, *Vice News*, and *BBC*. She is a frequent radio guest, appearing on National Public Radio shows, including *All Things Considered*, *WHYY's Radio Times*, *WNYC's Public Radio International*, *Minnesota Public Radio*, *WYPR's Midday with Dan Rodricks*, *Wisconsin Public Radio*, *WAMU's 1A*, *WAMU's The Diane Rehm Show*, and *Chicago Public Radio*.

Mr. DOYLE. Thank you very much.
The Chair now recognizes Dr. McSherry for 5 minutes.

STATEMENT OF CORYNNE MCSHERRY, PH.D.

Dr. MCSHERRY. Thank you.

As legal director for the Electronic Frontier Foundation, I want to thank the chairs, ranking members, and members of the committee for the opportunity to share our thoughts with you today on this very, very important topic.

For nearly 30 years, EFF has represented the interests of technology users, both in court cases and in broader policy debates, to help ensure that law and technology support our civil liberties.

Like everyone in this room, we are well aware that online speech is not always pretty. Sometimes it is extremely ugly and it causes serious harm. We all want an internet where we are free to meet, create, organize, share, debate, and learn. We want to have control over our online experience and to feel empowered by the tools we use. We want our elections free from manipulation and for women and marginalized communities to be able to speak openly about their experiences.

Chipping away at the legal foundations of the internet in order to pressure platforms to better police the internet is not the way to accomplish those goals.

Section 230 made it possible for all kinds of voices to get their message out to the whole world without having to acquire a broadcast license, own a newspaper, or learn how to code. The law has thereby helped remove much of the gatekeeping that once stifled social change and perpetuated power imbalances, and that is because it doesn't just protect tech giants. It protects regular people.

If you forwarded an email, a news article, a picture, or a piece of political criticism, you have done so with the protection of Section 230. If you have maintained an online forum for a neighborhood group, you have done so with the protection of Section 230. If you used Wikipedia to figure out where George Washington was born, you benefited from Section 230. And if you are viewing online videos documenting events realtime in northern Syria, you are benefiting from Section 230.

Intermediaries, whether social media platforms, news sites, or email forwarders, aren't protected by Section 230 just for their benefit. They are protected so they can be available to all of us.

There is another very practical reason to resist the impulse to amend the law to pressure platforms to more actively monitor and moderate user content. Simply put, they are bad at it. As EFF and many others have shown, they regularly take down all kinds of valuable content, partly because it is often difficult to draw clear lines between lawful and unlawful speech, particularly at scale, and those mistakes often silence the voices of already marginalized people.

Moreover, increased liability risk will inevitably lead to overcensorship. It is a lot easier and cheaper to take something down than to pay lawyers to fight over it, particularly if you are a smaller business or a nonprofit.

And automation is not the magical solution. Context matters very often when you are talking about speech, and robots are pretty bad at nuance.

For example, in December 2018, blogging platform Tumblr announced a new ban on adult content. In an attempt to explain the policy, Tumblr identified several types of content that would still be acceptable under the new rules. Shortly thereafter, Tumblr's own filtering technology flagged those same images as unacceptable.

Here is the last reason: New legal burdens are likely to stifle competition. Facebook and Google can afford to throw millions at moderation, automation, and litigation. Their smaller competitors or would-be competitors don't have that kind of budget. So, in essence, we would have opened the door to a few companies and then slammed that door shut for everyone else.

The free and open internet has never been fully free or open, and the internet can amplify the worst of us as well as the best. But at root, the internet still represents and embodies an extraordinary idea: that anyone with a computing device can connect with the world to tell their story, organize, educate, and learn. Section 230 helps make that idea a reality, and it is worth protecting.

Thank you, and I look forward to your questions.
[The prepared statement of Dr. McSherry follows:]



**The Subcommittee on Communications and Technology and the Subcommittee on Consumer
Protection and Commerce of the Committee on Energy and Commerce**

**Joint Hearing:
“Fostering a Healthier Internet to Protect Consumers”**

**Statement of Corynne McSherry, Ph.D.
Legal Director
Electronic Frontier Foundation**

October 16, 2019



As Legal Director for the Electronic Frontier Foundation, I thank Chairman Pallone, Ranking Member Walden and Members of the Subcommittee on Communications and Technology and the Subcommittee on Consumer Protection and Commerce for the opportunity to share EFF's views on how to create a healthier Internet and protect all of its users.

EFF is a donor-funded nonprofit, with contributions from more than 30,000 dues-paying members from around the world forming the backbone of our financial support. The majority of EFF's funding comes from ordinary individuals, and over 80% of that funding consists of donations under \$10,000. We receive less than six and a half percent of our funding from corporate sponsors.¹

For nearly 30 years, EFF has represented the interests of technology users both in court cases and in broader policy debates to help ensure that law and technology support our civil liberties. From that vantage point, we are well aware that online speech is not always pretty—sometimes it's extremely ugly and causes real-world harm. The effects of this kind of speech are often disproportionately felt by communities for whom the Internet has also provided invaluable tools to organize, educate, and connect. Systemic discrimination does not disappear and can even be amplified online. Given the paucity and inadequacy of tools for users themselves to push back, it's no surprise that many would look to Internet intermediaries to do more to limit such speech.

We all want an Internet where we are free to meet, create, organize, share, associate, debate, and learn. We want to make our voices heard in the way that technology now makes possible and to feel safe. We want to exercise control over our online environments and to feel empowered by the tools we use. We want our elections free from manipulation and for the speech of women and marginalized communities not to be silenced by harassment.

Chipping away at the legal foundations of the Internet is not the way to accomplish those goals. Instead, it is likely to backfire, to the detriment of all users but particularly to those who are most vulnerable to other forms of silencing. As a civil liberties organization, the Electronic Frontier Foundation's primary reason for defending Section 230 is the role that the law has played in providing a megaphone to those who previously lacked one, and removing much of the gatekeeping that stifled social change, perpetuated power imbalances, and rendered marginalized voices susceptible to censorship. Section 230 enables the existence of intermediaries that allow marginalized voices to get their messages out to the whole world, without having to own a printing press or a broadcast license, and without knowing how to code. It allows people to connect with people from around the world, to find community, organize, and advocate.

But Section 230 does far more. If you have ever forwarded an email—whether a news article, a party invitation, or a birth announcement—you have done so with the protection of Section 230. If you have ever maintained an online forum for a neighborhood group, you have done so with the

¹ 2018 Annual Report, Electronic Frontier Found. <https://www.eff.org/files/annual-report/2018>.



protection of Section 230. If you are a library that provides a forum for reader reviews, or a local newspaper that allows readers to comment online regarding the news of the day, or a job board that allows former employees to share comments about a prospective company, you do so with the protection of Section 230. If you’ve used Wikipedia to figure out the birthplace of George Washington or the airspeed velocity of an unladen swallow, you have benefited (indirectly) from Section 230. When you watch online videos documenting events in real time in northern Syria, you are benefiting from Section 230.

To be clear, the free and open Internet has never been fully free or open. And it can amplify the worst of us as well as the best. But at root, the Internet still represents and embodies an extraordinary idea: that anyone with a computing device can connect with the world, anonymously or not, to tell their story, organize, educate, and learn. Section 230 helps make that idea a reality. And it is still worth protecting.

A. What Section 230 Does

Commonly referred to as Section 230, 47 U.S.C. § 230 originated in H.R. 1978—the “Internet Freedom and Family Empowerment Act”—introduced in 1995 by Reps. Chris Cox (R-CA) and Ron Wyden (D-OR)—but was ultimately incorporated into the Telecommunications Act of 1996.

Section 230 provides broad—but not absolute—immunity for Internet intermediaries from legal liability for user-generated content. 47 U.S.C. § 230(c)(1) states that “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”

This means Internet intermediaries that host third-party content are protected against a range of laws that might otherwise be used to hold them legally responsible for what their users say and do. Specifically, Section 230 provides immunity to platforms against liability under state law—whether criminal or civil—and against liability under federal civil law, but not under federal criminal law or copyright law.

At the same time, Section 230 protects companies when they choose to moderate their platforms. Indeed, part of the genesis of the law was a pair of defamation disputes where one company was held liable for content on its service, and the other was not, because the first company chose to moderate generally but failed to catch the defamatory statement. Section 230 remedied that disparity, providing a safe harbor for moderation.²

In essence, Section 230 ensures that while Internet platforms—ISPs, web hosting companies, webmail providers, blogging platforms, social media and review sites, online marketplaces, photo

² *CDA 230: Legislative History*, Electronic Frontier Found. <https://www.eff.org/issues/cda230/legislative-history>.



and video sharing platforms, and cloud storage providers—have limited liability for the speech on their platforms, they are also free to remove or restrict users or speech that have violated their standards or terms of service.

B. What Section 230 Does Not Do

It's also important to understand what Section 230 does *not* do. Section 230 has important exceptions: it doesn't provide immunity against prosecutions under federal criminal law, liability based on intellectual property law, electronic communications privacy law, or certain sex trafficking laws. For example, a federal judge in the Silk Road case correctly ruled that Section 230 did not provide immunity against federal prosecution to the operator of a website that hosted other people's ads for illegal drugs.³

Courts have also held that Section 230 does not provide immunity against civil or state criminal liability where the company had a direct role in creating the content at issue or where liability is otherwise based on the company's own actions, rather than on user-generated content. For example:

- In *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, the Ninth Circuit held that Roommates.com could not claim immunity under Section 230 where it required users to choose among set answers to questions that violated anti-discrimination laws.⁴
- In *Anthony v. Yahoo!, Inc.*, a district court held that Section 230 did not apply to claims against Yahoo! based on the company's own creation of false dating profiles and its tactic of sending users now-defunct profiles in order to entice them to re-subscribe.⁵ Similarly, the Fourth Circuit explained in *Nemet Chevrolet, LTD. v. ConsumerAffairs.com, Inc.* that Section 230 would not apply to claims that a platform had fabricated reviews of a plaintiff's business.⁶
- In *Barnes v. Yahoo!, Inc.*, the Ninth Circuit held that Section 230 did not bar a claim against Yahoo! based on the company's failure to take down a false profile of the plaintiff *after* a company employee assured her that it would be removed. The reason is that claim was based on Yahoo!'s failure to honor its promise to the plaintiff, not the user-generated content itself.⁷

³ Cyrus Farivar, *Judge denies Silk Road's demands to dismiss criminal prosecution*, Ars Technica (July 9, 2014), <https://arstechnica.com/tech-policy/2014/07/judge-denies-silk-roads-demands-to-dismiss-criminal-prosecution>.

⁴ *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008).

⁵ *Anthony v. Yahoo! Inc.*, 421 F.Supp.2d 1257 (N.D. Cal. 2006).

⁶ *Nemet Chevrolet, LTD. v. ConsumerAffairs.com, Inc.*, 591 F.3d 250 (4th Cir. 2009).

⁷ *Barnes v. Yahoo!*, 570 F.3d 1096 (9th Cir. 2009).



- In *Doe v. Internet Brands, Inc.*, the Ninth Circuit held that Section 230 did not immunize a networking website from a “failure to warn” claim brought by one of its users who posted content to its site, because the plaintiff’s claims did not derive from her content, but rather Internet Brands’ own actions.⁸

Thus, Section 230’s safe harbor, while substantial, is significantly narrower than is often supposed.

Another common misconception is that Section 230 provides special legal protection only to “tech companies.”⁹ For example, legacy news media companies often complain that Section 230 gives online social media platforms extra legal protections and thus an unfair advantage. In fact, Section 230 makes no distinction between news entities and social media platforms. When a news media entity operates online, it gets the exact same Section 230 immunity from liability based on someone else’s content as a social media platform does. So, for example, news media entities have Section 230 immunity from any liability that arises from online comments that readers post to articles, or wire service stories or advertisements run online.¹⁰ Conversely, a big tech company is *not* protected by Section 230 when it publishes someone else’s content in print. That means, for example, that Airbnb can’t use Section 230 to avoid liability based on user reviews or letters to the editor that it might publish in its new print magazine.¹¹

Nor is Section 230’s protection limited to businesses. Instead, it provides immunity to any “provider *or* user of an interactive computer service” when that “provider or user” republishes content created by someone or something else. “User,” in particular, has been interpreted broadly to apply “simply to anyone using an interactive computer service.”¹²

Finally, it bears repeating that Section 230 does not prevent Internet companies from removing unlawful or objectionable content.¹³ To the contrary, as noted above, it encourages them to do so by protecting them from liability for actions “taken in good faith to restrict access or availability” of material they deem objectionable. To be clear, however, they do not have to do so in a “neutral”

⁸ *Doe v. Internet Brands, Inc.*, 824 F.3d 846 (9th Cir. 2016).

⁹ David Greene, *Section 230 Is Not A Special “Tech Company” Immunity*, Electronic Frontier Found. (May 1, 2019), <https://www.eff.org/deeplinks/2019/04/section-230-not-special-tech-company-immunity>.

¹⁰ Eric Goldman, *Yet Another Case Says Section 230 Immunizes Newspapers from User Comments—Hadley v. GateHouse Media*, Technology & Marketing Law Blog (July 15, 2012), https://blog.ericgoldman.org/archives/2012/07/yet_another_cas.htm.

¹¹ *See the world through a local lens*, Airbnb magazine, <https://www.airbnb.com/magazine>.

¹² *Barrett v. Rosenthal*, 40 Cal. 4th 33 (2006).

¹³ Mike Masnick, *Wired’s Big Cover Story On Facebook Gets Key Legal Point Totally Backwards, Demonstrating Why CDA 230 Is Actually Important*, TechDirt (Feb. 20, 2012), <https://www.techdirt.com/articles/20180216/16165239254/wireds-big-cover-story-facebook-gets-key-legal-point-totally-backwards-demonstrating-why-cda-230-is-actually-important.shtml>.



manner;¹⁴ any such requirement would violate the First Amendment, which gives online platforms the choice about what speech they will and will not host.

C. Section 230 Helps Ensure the Internet’s Growth as a Platform for Speech and Innovation

Section 230 has ushered in a new era of community and connection on the Internet. People can find friends old and new over the Internet, learn, share ideas, organize, and speak out. Those connections can happen organically, often with no involvement on the part of the platforms where they take place. Consider that some of the most vital modern activist movements—#MeToo, #WomensMarch, #BlackLivesMatter—are universally identified by hashtags.

The ways in which the Internet has grown as a platform for everyone to speak out go far beyond what lawmakers had imagined when they wrote Section 230. The freedom that Section 230 afforded to Internet startups to choose their own moderation strategies has led to a multiplicity of options for users—some more restrictive and sanitized, some more *laissez-faire*. That mix of moderation philosophies contributes to a healthy environment for free expression and association online.¹⁵

Indeed, and perhaps ironically, Section 230 has also played a key role in the development of Internet filtering technologies and practices. While the technologies platforms use to find offensive speech remain deeply flawed, they’ve been allowed to evolve under the legal protections of Section 230.¹⁶ Without those protections, the extremely high risk associated with letting a piece of unlawful content slip by would have discouraged platforms from improving them, and the filters on the market today would look much like notoriously flawed “parental control” tools of the 1990s.¹⁷

Section 230 also plays an important role in preventing or limiting efforts to use legal threats to silence critics. Defamation law in particular is already frequently abused to silence and intimidate critics, including using legal process to unmask anonymous speakers solely for purposes of retaliation.¹⁸ Without Section 230, bad-faith actors could wield these tactics equally effectively against not only the original author of the criticism but also anyone who forwards it, quotes it, or

¹⁴ Elliot Harmon, *No, Section 230 Does Not Require Platforms to Be “Neutral”*, Electronic Frontier Found. (Apr. 12, 2018), <https://www.eff.org/deeplinks/2018/04/no-section-230-does-not-require-platforms-be-neutral>.

¹⁵ Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendants-Appellees and Affirmation, *Prager University v. Google*, No. 18-15712 (9th Cir. Nov. 7, 2018), <https://www.eff.org/document/prager-university-v-google-eff-amicus-brief>.

¹⁶ Carl Szabo, *Section 230 Is the Internet Law That Stops the Spread of Extremist and Hate Speech*, Morning Consult (Aug. 27, 2019), <https://morningconsult.com/opinions/section-230-is-the-internet-law-that-stops-the-spread-of-extremist-and-hate-speech>.

¹⁷ Jonathan Weinberg, *Rating the Net*, 19 Hastings Comm. & Ent. L.J. 453 (1996), https://repository.uchastings.edu/hastings_comm_ent_law_journal/vol19/iss2/5

¹⁸ cyberSLAPP.org, <http://www.cyberslapp.org>.



otherwise shares it online. For example, Section 230 unambiguously provides Rose McGowan immunity from defamation liability for sharing, via Twitter, stories that other women sent her about abuse by Harvey Weinstein.

But Section 230's beneficial effect is even more pervasive. A host of ordinary activities depend on Section 230's protections. Users can forward an email without worrying whether its contents might be deemed defamatory under some state's law. A library can host an online catalog that allows for reader reviews. A university can provide forums for students to share their work. A job search service can allow employees to share their views on a given employer. Wikipedia can offer a free online encyclopedia used by everyone from schoolchildren to judges.¹⁹ And so on.

Section 230 was crafted before many of these services and activities existed, and it's easy to forget that it gives them legal shelter. In fact, for people who rely on online communities and services to share ideas, knowledge, and culture, Section 230 is more crucial today than ever before.

D. Proceed with Caution: The Risks of Undermining Section 230

1. Weakened Liability Protections Will Undermine Valuable Online Speech

a) Increased Liability Risk Will Lead to Over-censorship

Without Section 230—or with a weakened Section 230—online platforms would have to exercise extreme caution in their moderation decisions in order to limit their own liability. A platform with a large number of users can't remove all unlawful speech while keeping everything else intact. Therefore, undermining Section 230 effectively forces platforms to put their thumbs on the scale—that is, to remove far more speech than only what is actually unlawful, censoring innocent people and often important speech in the process.

The effects of 2018's Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) offer an object lesson. FOSTA amended Section 230 to create new civil and criminal liability for platforms that host content about sex work at both the state and federal levels. It also broadly and ambiguously expanded federal criminal law to target online platforms where users discuss sex work and related topics.

FOSTA's impact on Internet speech was apparent almost immediately after the law passed. Internet companies became significantly more restrictive toward speech discussing sex.²⁰ The law threw harm reduction activities in the sex work community into a legal gray area, giving the organizations providing support to sex workers the unpleasant choice of taking on a great deal of

¹⁹ Leighanna Mixer, *Three Principles in CDA 230 That Make Wikipedia Possible*, Wikimedia Found. (Nov. 9, 2017) <https://blog.wikimedia.org/2017/11/09/cda-230-principles-wikipedia>.

²⁰ Elliot Harmon, *Facebook's Sexual Solicitation Policy is a Honeytrap for Trolls* (Dec. 7, 2018), <https://www.eff.org/deeplinks/2018/12/facebooks-sexual-solicitation-policy-honeytrap-trolls>.



legal risk or ceasing operations.²¹ Unfortunately, many of them chose the latter. Websites that sex workers relied on for sharing information about dangerous clients have gone offline, putting sex workers' lives at risk.²²

At the same time, platforms presented with new liability risks immediately moved to over-censor. For example, Craigslist completely removed its message boards dedicated to both personal ads and therapeutic services. The company could not individually review every post on those boards—and even if it could, it would not be able to reliably recognize every unlawful post—so it removed the boards altogether, punishing legitimate, lawful businesses in the process.²³ Similarly, Tumblr—a community which many LGBTQ users have said was vital to them as youth²⁴—chose to ban all sexual content. Some smaller, niche personals sites either removed certain features or closed entirely.²⁵

Our founders knew that it is impossible to craft laws that only target bad actors, which is why the First Amendment protects most speech, even distasteful or “indecent” speech. Private enforcers face the same problem, and it will only worsen if a failure to enforce perfectly could lead to legal liability.

b) The Content Moderation System is Already Broken

For decades, EFF has followed the role of social media companies in providing platforms for users to speak and exchange ideas, including the recent surge in “voluntary” platform censorship.

That surge drew public attention in 2017 when a company called Cloudflare made headlines for its decision to take down a neo-Nazi website called *The Daily Stormer*.²⁶ But that was far from the only instance. Two years ago, for example, YouTube came under fire for restricting LGBTQ content.²⁷ Companies—under pressure from lawmakers, shareholders, and the public alike—

²¹ Karen Gullo and David Greene, *With FOSTA Already Leading Censorship, Plaintiffs Are Seeking Reinstatement Of Their Lawsuit Challenging the Law's Constitutionality* (March 1, 2019), <https://www.eff.org/deeplinks/2019/02/fosta-already-leading-censorship-we-are-seeking-reinstatement-our-lawsuit>

²² Emily McCombs, *'This Bill Is Killing Us': 9 Sex Workers On Their Lives In The Wake Of FOSTA* (May 11, 2018), https://www.huffpost.com/entry/sex-workers-sesta-fosta_n_5ad0d7d0e4b0edca2cb964d9

²³ Karen Gullo and David Greene, *With FOSTA Already Leading Censorship, Plaintiffs Are Seeking Reinstatement Of Their Lawsuit Challenging the Law's Constitutionality* (March 1, 2019), <https://www.eff.org/deeplinks/2019/02/fosta-already-leading-censorship-we-are-seeking-reinstatement-our-lawsuit>

²⁴ Prodi Sabarini, *Why Tumblr's ban on adult content is bad for LGBTQ youth*, *The Conversation* (Dec. 6, 2018), <https://theconversation.com/why-tumblrs-ban-on-adult-content-is-bad-for-lgbtq-youth-108215>

²⁵ *Documenting Tech Actions*, *Survivors Against SESTA*, <https://survivorsagainstsesta.org/documentation/>

²⁶ Jeremy Malcolm, Cindy Cohn & Danny O'Brien, *Fighting Neo-Nazis and the Future of Free Expression*, Electronic Frontier Found. (Aug. 17, 2017), <https://www.eff.org/deeplinks/2017/08/fighting-neo-nazis-future-free-expression>

²⁷ Catherine Shu, *YouTube updates its policies after LGBTQ videos were blocked in Restricted Mode*, *TechCrunch* (Jun. 19, 2017), <https://techcrunch.com/2017/06/19/youtube-updates-its-policies-after-lgbtq-videos-were-blocked-in-restricted-mode>.



ramped up restrictions on speech, adding new rules,²⁸ adjusting their still-hidden algorithms, and hiring more staff to moderate content.²⁹ They have banned ads³⁰ from certain sources and removed “offensive” but legal content.³¹

All of these efforts have, predictably, led to the silencing of all kinds of lawful speech. For example, social media platforms have been hard-pressed to remove violent extremism while keeping videos and other content *documenting* violent extremism intact.³² We’ve seen prohibitions on hate speech employed to silence individuals engaging in anti-racist speech³³ and rules against harassment used to suspend the account of an activist calling out their harasser.³⁴

These mistakes are the result, in part, of an intractable problem: threats to free expression in real life and on the Internet don’t always come in obvious packages, announcing their presence. They instead may come in the form of speech—describing hateful violence, aggression and despicable acts—that fair-minded people find appalling. The desire to remove this speech (and hopefully, the underlying prejudice) from public discourse is understandable, but fulfilling that desire is likely to lead to a host of unintended consequences for all online speech. Those on the left face calls³⁵ to characterize the Black Lives Matter movement as a hate group. In the Civil Rights Era cases that formed the basis of today’s protections for freedom of speech, the NAACP’s voice was the one attacked.³⁶

²⁸ Sarah Perez, *Twitter posts a new version of its rules with updated sections on abuse, spam, violence, and more*, TechCrunch (Nov. 3, 2017), <https://techcrunch.com/2017/11/03/twitter-posts-a-new-version-of-its-rules-with-updated-sections-on-abuse-spam-violence-and-more>.

²⁹ Colin Lecher, *Facebook will add 3,000 moderators after video killings*, The Verge (May 3, 2017), <https://www.theverge.com/2017/5/3/15529864/facebook-mark-zuckerberg-violence-moderation-reviewers>.

³⁰ Natasha Bertrand, *Twitter is banning all ads from Russian news agencies RT and Sputnik effective immediately*, Bus. Insider (Oct. 26, 2017), <http://www.businessinsider.com/twitter-is-banning-all-ads-from-russian-news-agencies-rt-and-sputnik-2017-10>.

³¹ Jason Kelley & Jillian York, *Seven Times Journalists Were Censored: 2017 in Review*, Electronic Frontier Found. (Dec. 30, 2017), <https://www.eff.org/deeplinks/2017/12/seven-times-2017-journalists-were-censored>.

³² Abdul Rahman Al Jaloud, Hadi Al Khatib, Jeff Deutch, Dia Kayyali, and Jillian C. York, *Caught in the Net: The Impact of “Extremist” Speech Regulations on Human Rights Content*, Electronic Frontier Found. (May 30, 2019), <https://www.eff.org/wp/caught-net-impact-extremist-speech-regulations-human-rights-content>.

³³ Natalie Wiener, *Talib Kweli Calls Out Instagram for Deleting His Anti-Racism Post*, Billboard (July 1, 2015), <https://www.billboard.com/articles/columns/the-juice/6613208/talib-kweli-instagram-deleted-post-anti-racism-censorship>.

³⁴ Kaitlyn Tiffany, *Twitter criticized for suspending popular LGBTQ academic @meakoopa*, The Verge, (Jun 13, 2017), <https://www.theverge.com/2017/6/13/15794296/twitter-suspended-meakoopa-anthony-oliveira-controversy>.

³⁵ Richard Cohen, *Black Lives Matter is Not a Hate Group*, Southern Poverty Law Center, July 16, 2016, <https://www.splcenter.org/news/2016/07/19/black-lives-matter-not-hate-group>.

³⁶ David Greene and Shahid Buttar, *The Inextricable Link Between Modern Free Speech Law and the Civil Rights Movement*, Electronic Frontier Found. (March 8, 2019), <https://www.eff.org/deeplinks/2019/03/inextricable-link-between-modern-free-speech-law-and-civil-rights-movement>.



c) *Moderation Decisions Often Privilege the Powerful*

In addition, moderation choices often reflect and reinforce bias against marginalized communities. Indeed, for every high-profile case of despicable content being taken down, there are many more stories of people in marginalized communities and journalists finding their voices silenced online. Here are just a few examples:

- Instagram often deletes photos of transgender people and people of color while keeping nearly identical photos of white, cisgender people online.³⁷ *Salty*, a lifestyle magazine for women, transgender, and nonbinary readers, attempted to advertise on Instagram but had its advertisements rejected, apparently due to a misapplication of a rule banning advertisements for escort services.³⁸
- Under rules against online harassment, platforms frequently mistakenly punish the targets of harassment who are attempting to engage in counter-speech, rather than the perpetrators.³⁹
- Flickr removed photos of Egypt's state security force from a user's account claiming the takedown was because the user did not create the images himself.⁴⁰
- Facebook allows white supremacists to spread violent threats while censoring Black Lives Matter posts and activists of color.⁴¹
- Twitter regularly removes ads related to sexual health and condoms but allows Playboy to promote its account freely.⁴²
- Egyptian journalist Wael Abbas has been censored by Facebook, Yahoo!, Twitter, and YouTube in connection with his work documenting police brutality.⁴³

³⁷ EJ Dickson, *Why Did Instagram Confuse These Ads Featuring LGBTQ People for Escort Ads?*, Rolling Stone (July 11, 2019), <https://www.rollingstone.com/culture/culture-features/instagram-transgender-sex-workers-857667>.

³⁸ Mary Emily O'Hara, *Queer and Feminist Brands Say They are Being Blocked from Running Ads on Instagram and Facebook*, MTV News (July 19, 2019), <http://www.mtv.com/news/3131929/queer-and-feminist-brands-say-they-are-being-blocked-from-running-ads-on-instagram-and-facebook>.

³⁹ Katie Notopoulos, *How Trolls Locked My Twitter Account for 10 Days, and Welp*, BuzzFeed News (Dec. 2, 2017), <https://www.buzzfeednews.com/article/katienotopoulos/how-trolls-locked-my-twitter-account-for-10-days-and-welp>; Elliot Harmon, *In debate over internet speech law, pay attention to whose voices are ignored*, The Hill (Aug. 21, 2019), <https://thehill.com/opinion/technology/458227-in-debate-over-internet-speech-law-pay-attention-to-whose-voices-are>.

⁴⁰ Jennifer Preston, *Ethical Quandary for Social Sites*, New York Times (Mar. 27, 2011), <https://www.nytimes.com/2011/03/28/business/media/28social.html>.

⁴¹ Sam Levin, *Civil rights groups urge Facebook to fix 'racially biased' moderation system*, The Guardian (Jan. 18, 2017), <https://www.theguardian.com/technology/2017/jan/18/facebook-moderation-racial-bias-black-lives-matter>; Sam Levin, *Facebook temporarily blocks Black Lives Matter activist after he posts racist email*, The Guardian (Sept. 12, 2016), <https://www.theguardian.com/technology/2016/sep/12/facebook-blocks-shaun-king-black-lives-matter>.

⁴² Amber Madison, *When Social-Media Companies Censor Sex Education*, The Atlantic (Mar. 4, 2015), <https://www.theatlantic.com/health/archive/2015/03/when-social-media-censors-sex-education/385576>.

⁴³ Jillian C. York, *Companies Must Be Accountable to All Users: The Story of Egyptian Activist Wael Abbas* (Feb. 13, 2018), <https://www.eff.org/deeplinks/2018/02/insert-better-title-here>.



- YouTube removed reports about the Syrian war because of rules against depictions of violence.⁴⁴
- Facebook removed posts about the military campaign against the Rohingya in Myanmar.⁴⁵
- Facebook also removed links on a small news weekly's page to an opinion column criticizing men for their complacency in light of several high-profile sexual assault and harassment scandals.⁴⁶

Problematically, companies' moderation policies also often feature exceptions for public figures: that's why the president of the United States can post false information but an ordinary user can't. While there's some sense to such policies—people should know what their elected representatives are saying—they necessarily privilege the powerful.⁴⁷

Given this background, we worry that the users most likely to be harmed by a weakened Section 230 are the people who most rely on online communities to safely gather and share information: racial and religious minorities, members of the LGBTQ community, and other marginalized groups. For some of those groups, online platforms provide safety and resources that aren't available anywhere else. As a group of South Dakota activists wrote in a letter to Senator John Thune:

[Section 230's] protections are uniquely important to South Dakotans: we rely on online communities to share our thoughts and ideas with friends across the country and around the world. For rural Americans, online communities often serve as our most important connection to likeminded friends. For people of color, members of the LGBTQ community, and other marginalized South Dakotans, online communities are our lifelines.⁴⁸

Online platforms can give power to the most vulnerable members of society. As EFF Chief Program Officer Rainey Reitman put it, "Online communities let women make decisions from the safety of our homes about whom we can trust. When we're forced to make those decisions on the

⁴⁴ Malachy Browne, *YouTube Removes Videos Showing Atrocities in Syria*, New York Times (Aug. 22, 2017), <https://www.nytimes.com/2017/08/22/world/middleeast/syria-youtube-videos-isis.html>.

⁴⁵ *Facebook Bans Rohingya group's Posts as Minority Faces 'Ethnic Cleansing.'* The Guardian (Sept. 20, 2017), <https://www.theguardian.com/technology/2017/sep/20/facebook-rohingya-muslims-myanmar>.

⁴⁶ Jillian C. York, *Blunt Measures on Speech Serve No One: The Story of the San Diego City Beat* (Mar. 5, 2018), <https://www.eff.org/deeplinks/2018/03/blunt-measures-speech-serve-no-one-story-san-diego-city-beat>.

⁴⁷ Kit Walsh and Jillian C. York, *Facebook Shouldn't Give Politicians More Power Than Ordinary Users*, Electronic Frontier Found. (October 6, 2019), <https://www.eff.org/deeplinks/2019/10/facebook-shouldnt-give-politicians-more-power-ordinary-users>.

⁴⁸ Elliot Harmon, *South Dakota Civil Liberties Groups Urge Senator Thune to Put the Brakes on SESTA*, Electronic Frontier Found. (Oct. 17, 2017), <https://www.eff.org/deeplinks/2017/10/south-dakota-civil-liberties-groups-urge-senator-thune-put-brakes-sesta>.



street, we're usually doing it from the wrong side of a power imbalance."⁴⁹ A weakened Section 230 means an Internet where some members of society aren't afforded that safety.

d) *The Robots Won't Fix It*

The situation worsens when we look to automation and algorithms to help enforce already confused policies. Machine learning algorithms are meant to grow and evolve on their own without human input, and they inevitably end up removing legal and often important speech.

For example, when Google launched its PerspectiveAPI tool, designed to measure the "toxicity" in online discussions based on feedback from users, users quickly noticed troubling results in how it would treat different user demographics, flagging statements like "I am a gay woman" and "I am a black man" as highly toxic.⁵⁰ And when blogging platform Tumblr turned to automated tools last year to enforce its ban on "adult" content, its filters flagged a wide variety of non-adult content, including images Tumblr itself has identified as acceptable and even ordinary drawings from patent applications.⁵¹

Automation failures can have significant consequences for human rights. In Syria, human rights defenders have found the openness of the YouTube platform to be a major benefit to their efforts to document the conflict. Syrian activists have relied on both YouTube and Facebook to generate more hours of content than the length of the conflict itself, some of which has been collected for use in war crimes tribunals. But YouTube's automated filters have taken down thousands of Syrian channels that depicted human rights violations. Our joint investigation with Syrian Archive and Witness estimates that at least 206,077 videos, including 381 videos documenting airstrikes targeting hospitals and medical facilities, have been removed from the platform between 2011 and 2019.⁵²

Political criticism also suffers. For example, a video by Kurdish activist was flagged simply because it contained imagery that depicted Turkey's President Erdogan as a member of ISIS.⁵³

⁴⁹ Rainey Reitman, *Commentary: Bill Aimed at Sex Trafficking Actually Puts Women in More Danger*, Mercury News (Dec. 11, 2017), <https://www.mercurynews.com/2017/12/11/commentary-bill-aimed-at-sex-trafficking-actually-puts-women-in-more-danger>.

⁵⁰ Elliot Harmon and Jeremy Gillula, *Whose Voices Will SESTA Silence?*, Electronic Frontier Found. (Sept. 13, 2017), <https://www.eff.org/deeplinks/2017/09/stop-sesta-whose-voices-will-sesta-silence>.

⁵¹ *What Tumblr's Ban on 'Adult Content' Actually Did*, Electronic Frontier Found. (Dec. 2018), <https://www.eff.org/tossedout/tumblr-ban-adult-content>.

⁵² Abdul Rahman Al Jaloud, Hadi Al Khatib, Jeff Deutch, Dia Kayyali, and Jillian C. York, *Caught in the Net: The Impact of "Extremist" Speech Regulations on Human Rights Content*, Electronic Frontier Found. (May 30, 2019), <https://www.eff.org/wp/caught-net-impact-extremist-speech-regulations-human-rights-content>.

⁵³ Sara Spary, *Facebook Is Embroiled In A Row With Activists Over "Censorship"*, BuzzFeed, (April 8, 2016) <https://www.buzzfeed.com/sarasparry/facebook-in-dispute-with-pro-kurdish-activists-over-deleted>.



And state actors have systematically abused Facebook’s flagging process to censor political enemies.⁵⁴

Further examples abound; EFF has documented a few of the most egregious ones in our “TOSsed Out” archive.⁵⁵

Building a more complicated filter—say, by using advanced machine learning or AI techniques—won’t solve the problem either. That’s because all complex machine learning systems are susceptible to what are known as “adversarial inputs”—examples of data that look normal to a human, but which completely fool AI-based classification systems. For example, an AI-based filtering system that recognizes sex trafficking posts might look at such a post and classify it correctly—unless the sex trafficker adds some random-looking-yet-carefully-chosen characters to the post (maybe even a block of carefully constructed incomprehensible text at the end), in which case the filtering system will classify the post as having nothing to do with sex trafficking.⁵⁶

Based on the track record of filters for copyright infringement, these problems were unfortunately predictable. YouTube’s expensive and sophisticated Content ID system has a woeful track record at flagging noninfringing videos as copyright infringement,⁵⁷ including infamously flagging a video of nothing but static five times.⁵⁸ It is telling that even one of the most powerful Internet companies in the world, with powerful incentives, nonetheless still cannot filter reliably.

Finally, automated speech “decisions,” unlike those of courts, are often shrouded in mystery because the technology is hidden behind a veil of trade secrets and other assertions of proprietary information. When platforms like Facebook and YouTube create large databases of what they believe to represent “terrorist” content, the algorithm begins to define what it considers “terrorist” content to be, but few people in the human rights community, if any, have knowledge about how they’re programmed.⁵⁹ Fionnuala Ní Aoláin, a law professor and special rapporteur for the United Nations Human Rights Council, has been quoted as saying that Facebook’s definition of terrorism “bears no relationship to the global definition agreed by states,” a development which she sees as “a very dangerous precedent.”⁶⁰

⁵⁴ Russell Brandon, *Facebook’s Report Abuse Button has Become a Tool of Global Oppression*, The Verge (Sept 4, 2014), <https://www.theverge.com/2014/9/2/6083647/facebook-s-report-abuse-button-has-become-a-tool-of-global-oppression>.

⁵⁵ *TOSsed Out*, Electronic Frontier Found. <https://www.eff.org/tossedout>

⁵⁶ *Attacking Machine Learning with Adversarial Examples*, OpenAI (February 27, 2017) <https://openai.com/blog/adversarial-example-research>.

⁵⁷ Elliot Harmon, *Don’t Put Robots in Charge of the Internet*, Electronic Frontier Found. (Jan. 18, 2019), <https://www.eff.org/deeplinks/2019/01/dont-put-robots-charge-internet>.

⁵⁸ *Ten Hours of Static Gets Five Copyright Notices*, Electronic Frontier Found. (Jan. 4, 2018), <https://www.eff.org/takedowns/ten-hours-static-gets-five-copyright-notices>.

⁵⁹ Bernhard Warner, *Tech Companies Are Deleting Evidence of War Crimes*, The Atlantic (May 8, 2019), <https://www.theatlantic.com/ideas/archive/2019/05/facebook-algorithms-are-making-it-harder/588931>.

⁶⁰ *Id.*



Given the value we place on free speech and access to information in the United States, we should be wary of giving control over both to a network of robot Star Chambers.

2. Raising the Cost of Hosting 3rd Party Speech May Help Also Cement the Dominance of Big Tech

As noted, Section 230 has played a key role in the development of the today’s Internet industry. Without Section 230, Google, Facebook, and Twitter would not exist in their current form. It’s understandable that some people who are concerned about the outsized power of the tech giants are drawn toward proposals to modify Section 230.

Unfortunately, any such attempt is likely to backfire. If Section 230 does nothing else, it helps pave the way for competition. As Professor Eric Goldman of Santa Clara University School of Law puts it, “Even as Section 230 privileges the Internet giants, it also plants the seeds of their future destruction.”⁶¹

Simply put, Section 230 dramatically reduces the legal cost of hosting third-party speech. This allows Internet platforms both big and small, commercial and nonprofit, to operate at a global scale. Whether it’s Wikipedia, the world’s largest (and continuously growing) repository of information, staffed by a mere 350 people worldwide (approximately one third of the size of just Google’s legal department); or the Internet Archive’s 150 staff members that maintain an archive of the entire Internet on a budget of just \$18 million a year; these types of massive global efforts would not exist without a strong Section 230.

Eviscerating Section 230, or imposing new burdens in exchange for immunity, would make those operations untenable (much less the smaller operations of many startups, websites, and community forums). The tech giants, by contrast, would have resources to shoulder those burdens. They also have the legal resources to fight off the lawsuits a weakened Section 230 would invite.⁶² More generally, changing the formula after the fact only favors established companies that have used the law to establish a foothold while their would-be usurpers are forced to tread less certain legal waters. And if competing products don’t exist, users cannot simply switch services as a means to discipline a company’s conduct.

To see how this works now, we need only look to the example of the Grindr dating website, which was hardly a giant but was nonetheless financially successful. A subscriber misused the service as part of a harassment campaign targeting a former boyfriend, with terrible consequences for that

⁶¹ Eric Goldman, *Want to Kill Facebook and Google? Preserving Section 230 Is Your Best Hope*, Balkinization, New Controversies in Intermediary Liability Law (June 3, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3398631.

⁶² Elliot Harmon, *Google Will Survive SESTA. Your Startup Might Not*, Electronic Frontier Found. (Sept. 22, 2017), <https://www.eff.org/deeplinks/2017/09/google-will-survive-sesta-your-startup-might-not>



person. The victim sued Grindr, alleging it failed to do enough to help stop the harassment, and the lawsuit garnered intense press coverage. Even though Grindr was not found liable under Section 230, users looking for a safer experience turned to alternative dating applications committed to tougher vetting and safety processes.⁶³ Those competitors were just as dependent on 230's protections as they experimented with moderation techniques as Grindr itself was.

We do not have to guess as to whether the potential impacts on profits would be sufficiently motivating for corporations to censor speech. We are witnessing it in real time today as corporations with financial entanglements in China willfully stifle expression on behalf of the Chinese government in order to preserve their access to lucrative markets.⁶⁴ There is little difference between preserving opportunities to increase profits in more censorship-oriented markets and eliminating their exposure to liability to a weakened Section 230 in order to protect profits.

Finally, competitive effects are another reason Congress should avoid pushing platforms toward more reliance on automated filtering. The cost of building and using automated systems for removing content makes these tools inaccessible for startups. For example, YouTube's Content ID system cost the company approximately \$100 million.⁶⁵ For comparison, the Wikimedia Foundation (the organization that maintains Wikipedia and several other information-sharing tools) has an annual budget of \$80 million.⁶⁶

E. (Further) Lessons from FOSTA

EFF is a part of the legal team representing the plaintiffs who are seeking to have FOSTA declared unconstitutional.⁶⁷ They include two human rights organizations, a digital library, a sex work activist, and a certified massage therapist.

⁶³ Jon Shadel, *Grindr was the First Big Dating App for Gay Men. Now It's Falling Out of Favor*, Washington Post (Dec. 6, 2018), <https://www.washingtonpost.com/lifestyle/2018/12/06/grindr-was-first-big-dating-app-gay-men-now-its-falling-out-favor/>.

⁶⁴ Matt Kim, *Hearthstone Pro Banned by Blizzard After Calling for Hong Kong Liberation During Stream*, IGN News (Oct. 7, 2019), <https://www.ign.com/articles/2019/10/08/hearthstone-pro-calls-for-hong-kong-liberation-during-live-blizzard-interview>; Laura Wagner, *Internal Memo: ESPN Forbids Discussion of Chinese Politics When Discussing Daryl Morey's Tweet About Chinese Politics*, Deadspin (Oct. 8, 2019), <https://deadspin.com/internal-memo-espn-forbids-discussion-of-chinese-polit-1838881032>.

⁶⁵ Paul Sawers, *YouTube: We've invested \$100 million in Content ID and paid over \$3 billion to rightsholders*, VentureBeat (Nov. 7, 2018), <https://venturebeat.com/2018/11/07/youtube-weve-invested-100-million-in-content-id-and-paid-over-3-billion-to-rightsholders>.

⁶⁶ Wikimedia Foundation, Inc., *Financial Statements June 30, 2018 and 2017 (With Independent Auditors' Report Thereon)*, KPMG, (Sept. 26, 2018), https://upload.wikimedia.org/wikipedia/foundation/6/60/FY17-18_-_Independent_Auditors%27_Report.pdf.

⁶⁷ Karen Gullo and David Greene, *With FOSTA Already Leading to Censorship, Plaintiffs Are Seeking Reinstatement of Their Lawsuit Challenging the Law's Constitutionality*, Electronic Frontier Found., (Mar 1, 2019) <https://www.eff.org/deeplinks/2019/02/fosta-already-leading-censorship-we-are-seeking-reinstatement-our-lawsuit>.



All of those plaintiffs have one thing in common: thanks to FOSTA, their lawful speech and activities are now compromised. Woodhull Freedom Foundation and Human Rights Watch both advocate for decriminalization of sex work. While their advocacy is completely legal, FOSTA put them at risk. Alex Andrews works with several organizations to provide harm reduction resources to sex workers. Like Woodhull and Human Rights Watch, Ms. Andrews' work is legal, but thanks to FOSTA's broad prohibition on using the Internet to "support" sex work, has now been thrown into a legal gray area. Massage therapist Eric Koszyk advertised his services on Craigslist's therapeutic services section and has now lost a key income source.

But the plaintiffs have another thing in common: they represent the types of voices that were sadly missing from the congressional debate over FOSTA. Groups like Freedom Network USA and the Sex Workers Outreach Project—both national networks of frontline organizations working to reduce trafficking—expressed grave concerns that FOSTA would put trafficking victims in more danger.⁶⁸ But those groups weren't invited to speak to Congress, and neither were Mr. Koszyk or other business owners whose work would be threatened by the law.

FOSTA teaches that Congress should carefully consider the unintended consequences of this type of legislation, recognizing that any law that puts the onus on online platforms to discern and remove illegal posts will result in over-censorship. Most importantly, it should listen to the voices most likely to be taken offline.

FOSTA also teaches that removing distasteful speech online may not have the hoped-for impact. At this committee's hearing on November 30, 2017, Tennessee Bureau of Investigation special agent Russ Winkler explained that online platforms were the most important tool in his arsenal for catching sex traffickers.⁶⁹ One year later, there is anecdotal evidence that FOSTA has made it harder for law enforcement to find traffickers.⁷⁰ Indeed, several law enforcement agencies report that without these platforms, their work finding and arresting traffickers has hit a wall.⁷¹

This is not a new lesson. For example, while many have worried that playing violent video games lead to real-world violence, researchers have been unable to establish any causal link.⁷² Similarly,

⁶⁸ Elliot Harmon, *Sex Trafficking Experts Say SESTA Is the Wrong Solution*, Electronic Frontier Found. Oct. 3, 2017), <https://www.eff.org/deeplinks/2017/10/sex-trafficking-experts-say-sesta-wrong-solution>.

⁶⁹ Elliot Harmon, *Internet Censorship Bills Wouldn't Help Catch Sex Traffickers*, Electronic Frontier Found. (Dec. 5, 2017), <https://www.eff.org/deeplinks/2017/12/internet-censorship-bills-wouldnt-help-catch-sex-traffickers>

⁷⁰ Mike Masnick, *More Police Admitting That FOSTA/SESTA Has Made It Much More Difficult To Catch Pimps And Traffickers* (July 9, 2018), <https://www.techdirt.com/articles/20180705/01033440176/more-police-admitting-that-fosta-sesta-has-made-it-much-more-difficult-to-catch-pimps-traffickers.shtml>.

⁷¹ Alexandra Stassinopoulos, *Anti-trafficking law has unexpected consequences on sex work in Bay Area*, The Daily Californian (May 3, 2019), <https://www.dailyca.org/2019/05/03/anti-trafficking-law-has-unexpected-consequences-on-sex-work-in-bay-area>.

⁷² Ollie Barder, *New Study Shows That There Is No Link Between Violent Video Games And Aggression In Teenagers*, Forbes (Feb. 15, 2019), <https://www.forbes.com/sites/olliebarder/2019/02/15/new-study-shows-that-there-is-no-link-between-violent-video-games-and-aggression-in-teenagers/#468f2c26328e>.



before Congress takes steps to undermine Section 230 in the hopes that policing hateful speech will help reduce dangerous hateful activities, it should take care to examine the causal links, if any, so that it can legislate with a scalpel, not a hacksaw.

F. Remedies Exist Under Current Law That Do Not Conflict with 230

Critics of Section 230 often forget that the law already affords rights and remedies to victims of harmful speech when it causes injury. Arguments that the tools that disseminate speech such as Internet platforms, broadband providers, and applications must be held liable for the conduct of users wrongly discount this fundamental fact. A speaker who harms another is not free from the consequences of their actions.

In the infamous *Grindr* case mentioned above, for instance, the abuser was arrested two years ago under criminal charges of stalking, criminal impersonation, making a false police report, and disobeying a court order.⁷³ Backpage.com, a controversial website that was frequently cited in debates over FOSTA, was shut down by the FBI in April 2018—without any help from or need for FOSTA.⁷⁴

States have also crafted a whole range of laws that hold individuals personally responsible for their harmful conduct that make it clear there are consequences. There are state criminal penalties for both stalking and harassment and a whole panoply of civil and criminal statutes for conduct that causes physical harm to an individual. The courts can draft restraining orders that carry with them penalties for their violation. Many of these criminal laws also carry civil enforcement equivalents as well.

In addition to criminal charges, victims can use defamation, false light, intentional infliction of emotional distress, common law privacy, interference with economic advantage, fraud, anti-discrimination laws, and other civil causes of action to seek redress. They can also sue the platforms if the platform owner is itself creating the illegal content. But just as we do not hold telephone companies liable for crimes committed over the telecommunications system, Section 230 stands for the consistent proposition that building a tool that allows the dissemination of information should not result in liability for what other parties do with that tool.

To the extent Congress believes any currently existing remedies individuals may invoke are insufficient, we encourage the Committee to explore why they are insufficient and to carefully

⁷³ Tyler KingKade and Davey Alba, *A Man Sent 1,000 Men Expecting Sex And Drugs To His Ex-Boyfriend Using Grindr, A Lawsuit Says*, BuzzFeed News (Jan. 10, 2019), <https://www.buzzfeednews.com/article/tylerkingkade/grindr-herrick-lawsuit-230-online-stalking>.

⁷⁴ Tom Porter and Reuters, *Backpage Website Shut Down, Founder Charged with 93 Counts by FBI in Sealed Document*, (Apr. 7, 2018) <https://www.newsweek.com/sex-ads-website-backpagecom-co-founder-charged-after-fbi-raid-876333>.



consider the collateral impacts any new remedies would yield. But I caution this committee to understand that there will be no law that will do a perfect job preemptively at all times.

G. Conclusion

Unfortunately, regulation of much of our online expression, thought, and association has already been ceded to unaccountable executives and enforced by minimally-trained, overworked staff and hidden algorithms. Nonetheless, many, especially in policy circles, continue to push for companies to perfectly differentiate—magically and at scale—between speech that should be protected and speech that should be erased. If our experience has taught us anything, it is that we have no reason to trust the powerful—inside governments, corporations, or other institutions—to draw those lines, and every reason to expect that the line-drawing processes will be abused.

Fighting censorship—by governments, large private corporations, or anyone else—has been core to EFF’s mission for more than 25 years, not because we enjoy defending reprehensible content, but because we know that tools for censorship are more often *used by the powerful, against the powerless*.⁷⁵ And we are worried about proposals to force platforms to filter the content on their services not because there’s a slippery slope from judicious moderation to active censorship—but because *we are already far down that slope*. Congress should not take us any further.

⁷⁵ Cindy Cohn, *10+ Years of Activists Silenced: Internet Intermediaries’ Long History of Censorship*, Electronic Frontier Found. (Aug. 23, 2017), <https://www.eff.org/deeplinks/2017/08/10-years-activists-silenced-internet-intermediaries-long-history-censorship>.

Mr. DOYLE. Thank you, Dr. McSherry.
Ms. Peters, you are recognized for 5 minutes.

STATEMENT OF GRETCHEN PETERS

Ms. PETERS. Thank you.

Distinguished members of the subcommittee, it is an honor to be here today to discuss one of the premier security threats of our time, one that Congress is well positioned to solve.

I am the executive director of the Alliance to Counter Crime Online. Our team is made up of academics, security experts, NGOs, and citizen investigators who have come together to eradicate serious organized crime and terror activity on the internet.

I want to thank you for your interest in our research and for asking me to join the panel of witnesses here to testify. Like you, I hoped to hear the testimony of the U.S. Trade Representative, because keeping CDA 230 language out of America's trade agreements is critical to our national security.

Distinguished committee members, I have a long history of tracking organized crime and terrorism. I was a war reporter, and I wrote a book about the Taliban and the drug trade. That got me recruited by U.S. military leaders to support our intelligence community. I mapped transnational crime networks and terror networks for Special Operations Command, the DEA, and CENTCOM. In 2014, I received State Department funding to map wildlife supply chains, and that is when my team discovered that the largest retail markets for endangered species are actually located on social media platforms like Facebook and WeChat.

Founding the Alliance to Counter Crime Online, which looks at crime more broadly than just wildlife, has taught me the incredible range and scale of illicit activity happening online. It is far worse than I ever imagined. We can and must get this under control.

Under the original intent of CDA 230, there was supposed to be a shared responsibility between tech platforms, law enforcement, and organizations like ACCO. But tech firms are failing to uphold their end of the bargain. Because of broad interpretations by the courts, they enjoy undeserved safe harbor for hosting illicit activity.

Distinguished committee members, the tech industry may try and convince you today that most illegal activity is confined to the dark web, but that is not the case. Surface web platforms provide much the same anonymity, payment systems, and a much greater reach of people.

We are tracking illicit groups ranging from Mexican drug cartels to Chinese triads that have weaponized social media platforms, I am talking about U.S., publicly listed social media platforms, to move a wide range of illegal goods.

Now we are in the midst of a public health crisis, the opioid epidemic, which is claiming the lives of more than 60,000 Americans a year. But Facebook, the world's largest social media company, only began tracking drug activity, drug postings on its platform, last year, and within 6 months the firm identified 1.5 million posts selling drugs. That is what they admitted to removing. To put that in perspective, that is 100 times more postings than the notorious dark website the Silk Road ever carried.

Study after study by ACCO members and others have shown widespread use of Google, Twitter, Facebook, Reddit, YouTube to market and sell fentanyl, oxycodone, and other highly addictive, often deadly substances to U.S. consumers in direct violation of U.S. law, Federal law. Every major internet platform has a drug problem. Why? Because there is no law that holds tech firms responsible, even when a child dies buying drugs on an internet platform.

Tech firms play an active role in facilitating and spreading harm. Their algorithms, originally designed, well-intentioned, to connect friends, also help criminals and terror groups connect to a global audience. ISIS and other terror groups use social media, especially Twitter, to recruit, fundraise, and spread their propaganda.

The ACCO alliance, among others, includes an incredible team of Syrian archaeologists recording the online trafficking of thousands of artifacts plundered from ancient sites and sold in many cases by ISIS supporters. This is a war crime.

We are also tracking groups on Instagram, Google, and Facebook where endangered species are sold, items ranging from rhino horn and elephant ivory to live chimpanzees and cheetahs. In some cases, the size of these online markets is literally threatening species with extinction.

I could continue to sit here and horrify you all morning. Illegal dog fighting, live videos of children being sexually abused, weapons, explosives, human remains, counterfeit goods—it is all just a few clicks away.

Distinguished committee members, the tech industry routinely claims that modifying CDA 230 is a threat to freedom of speech. But CDA 230 is a law about liability, not freedom of speech. Please try and imagine another industry in this country that has ever enjoyed such an incredible subsidy from Congress, total immunity, no matter what harm their product brings to consumers.

Tech firms could have implemented internal controls to prevent illicit activity from occurring, but it was cheaper and easier to scale while looking the other way. They were given this incredible freedom, and they have no one to blame but themselves for squandering it.

We want to see reforms to the law to strip immunities for hosting terror and serious crime content, to regulate that firms must report crime and terror activity to law enforcement, and appropriations to law enforcement to contend with this data.

Distinguished committee members, if it is illegal in real life, it ought to be illegal to host it online. It is imperative we reform CDA 230 to make the internet a safer place for all.

Thank you very much.

[The prepared statement of Ms. Peters follows:]



TIME TO REFORM CDA230

Testimony to the House Subcommittee on Communication and Technology and the Subcommittee on Consumer Protection and Commerce.

Delivered at the 16 October 2019 Hearing entitled, "Fostering a Healthier Internet to Protect Consumers."

Testimony by Gretchen Peters, Executive Director

Alliance to Counter Crime Online, Washington DC



Chairman Doyle, Chair Schakowsky, Ranking Members Latta and McMorris Rodgers and members of the Subcommittees: It's an honor to be here today before you to discuss one of the premier security threats of our time, one that your committees are well-positioned to solve.

I am the executive director of the Alliance to Counter Crime Online.

Our alliance is made up of academics, security experts, NGOs and citizen investigators that have come together to push serious organized crime and terror activity off the Internet.

Under the original intent of CDA Section 230, there was to be a shared responsibility between tech platforms, law enforcement, and organizations like ACCO.

However, tech firms are failing to uphold their end of the bargain and, because of overly broad interpretations by the courts, tech firms now use CDA 230 as a shield instead of a sword.

Congress must modify CDA 230 and create legal and financial incentives to hold tech firms accountable when they are knowingly or negligently facilitating illegal activity.

I want to thank you for your interest in our research and for asking me to join the panel of witnesses testifying today. Like you, I had hoped to hear the testimony of U.S. Trade Representative, because keeping CDA 230 language out of America's trade agreements is critical to our national security. Unfortunately, he chose to turn down Chairman Pallone's invitation and keep the American people in the dark regarding language in trade agreements that has global implications.

I have a long history tracking organized crime and terrorism. For years I worked as a war reporter and wrote a book about the Taliban and the drug trade. As a result of this work, I was recruited by U.S. military leaders to support the intelligence community, where I mapped transnational crime networks for Special Operations Command, the DEA and CENTCOM. In 2014, I received funding from State Department to map wildlife supply chains. That's when my team discovered that the largest retail markets for endangered species are on social media platforms like Facebook and WeChat.

Founding the Alliance to Counter Crime Online has taught me the incredible range and scale of illicit activity happening online. It is far worse than even I ever imagined.

Distinguished members of the committee: The Internet is the new frontier for organized crime and terror groups. We MUST get this under control.

Illicit groups have weaponized social media for years now, taking advantage of a market infrastructure that is global, encrypted and highly lucrative.

The tech industry will try and convince you that illegal activity is confined to the dark web.

But surface web platforms provide much the same anonymity as the dark web, as well as payments infrastructure – and a far greater reach of people.

We are in the midst of a public health crisis – the opioid epidemic – which is claiming the lives of more than 60-thousand Americans every year.

Study after study by ACCO members and others have shown widespread use of Google, Twitter, Facebook and YouTube by an estimated 35-thousand illegal online pharmacies to market and sell fentanyl, oxycodone and other highly addictive, often deadly controlled substances to U.S. consumers, in direct violation of federal law.



Facebook, for example, only began tracking drug postings on its platform last year. Within six months, they identified 1.5 million posts selling drugs – and that's just what they caught.

To put that in perspective, that's 100 times more postings than the notorious Dark Website the Silk Road ever carried.

Facebook-owned Instagram is today an open marketplace for drug dealers to target teens, and the corporation has never released any data on the volume of drug content on the platform. ACCO researchers have also tracked drug sales on Google, Reddit and Twitter. It's everywhere.

Why? Because there is no law that holds tech firms responsible, even when a child dies buying drugs on an internet platform.

And it's not just drug trafficking. Tech firms are removing far less terror content than they claim. Rather, their algorithms connect terror groups like Al Qaeda and Hezbollah to their supporters faster than beleaguered moderators can remove them, and on a wider global scale than these groups could have reached on their own.

ISIS and other terror groups use social media to sell looted artifacts from areas in conflict. ACCO members include an incredible team of Syrian archaeologists recording the online trafficking of thousands of artifacts plundered from ancient sites in their homeland, a war crime under the Second Protocol of the 1954 Hague convention.

We're now tracking more than 2 million members in 100 active Facebook groups where brokers, including members of terrorist groups, offer loot-to-order services across the Middle East.

Our researchers have identified three additional extremist groups aside from ISIS that are profiting from the sale of stolen artifacts on Facebook and operating with impunity.

We're tracking groups on Twitter, Instagram, Google and Facebook where endangered species are sold – items ranging from rhino horn and ivory to live cheetahs and apes. In some cases, the size of these markets is literally threatening key species with extinction. Our research, for example, has shown that 70 percent of the annual illegal cheetah trade takes place on Facebook and Instagram.

The black market on social media is far more than just drugs, wildlife, and stolen antiquities. For users who want to watch illegal dog fighting, screen live videos of child exploitation, buy guns, human remains or counterfeit goods, it's all just a few clicks away.

We support calls for increased user privacy, but current encryption plans laid out by the tech industry will make media platforms even safer for criminals and terrorists.

The tech industry routinely claims that modifying CDA 230 is a threat to freedom of speech.

But CDA 230 is not a law about free speech. It's about liability.

Try and imagine another industry that has ever enjoyed such an incredible subsidy from Congress: total immunity no matter what harm their product brings to consumers.

Tech firms could have implemented internal controls to prevent illicit activity from occurring but it was cheaper and easier to scale by looking the other way. They were given this incredible freedom, and they have no one to blame but themselves for squandering it.

The "move fast break things" culture developed precisely because of CDA 230.



We want to see reforms to the CDA230 which will remove safe harbor for criminal and terror content. That means:

- Stripping immunities for hosting terror and serious crime content
- Putting the onus on tech firms to monitor their platforms;
- Regulating that firms must report crime and terror activity, along with full data about the users who uploaded it, to law enforcement;
- Appropriating resources to law enforcement to contend with this data.

Distinguished committee members, if it's illegal in real life, it should be illegal to host it online.

It is imperative that we reform CDA230 to make the Internet a safer place for all. Thank you.



Reports by ACCO submitted as testimony to the House Committee on Energy and Commerce
Subcommittees on Communications and Technology & Consumer Protection and Commerce

Narcotics

Dr. Nilda M. Garcia, "[The Dark Side of Social Media: The Case of the Mexican Drug War](#)," University of Miami, University of Miami Scholarly Repository, 12/2017.

Dr. Tim Mackey, Jiawei Li, Qing Xu, Neal Shah, "[A machine learning approach for the detection and characterization of illicit drug dealers on Instagram: Model evaluation study](#)," *J Med Internet Res*. 2019 Jun 15;21(6):e13803. doi: 10.2196/13803.

Dr. Tim Mackey, Kalyanam J. [Detection of illicit online sales of fentanyl via Twitter](#). F1000Res. 2017;6:1937.

Dr. Tim Mackey, Kalyanam J, Katsuki T, Lanckriet G. [Twitter-Based Detection of Illegal Online Sale of Prescription Opioid](#). *Am J. Pub Health*. 2017;107:1910-1915.

Dr. Tim. Mackey, Kalynama J, Klugman J, Kuzmenko E, Gupta R. [Solution to Detect, Classify, and Report Illicit Online Marketing and Sales of Controlled Substances via Twitter: Using Machine Learning and Web Forensics to Combat Digital Opioid Access](#). *J Med Internet Res*. 2018;20(4):e10029.

Dr. Tim Mackey. Opioids and the Internet: [Convergence of Technology and Policy to Address the Illicit Online Sales of Opioids](#). *Health Serv Insights*. 2018 14;11:117863291880099.

Antiquities

Dr. Amr al-Azm, Katie Paul, "[Facebook's Black Market in Antiquities](#)," ATHAR Project, June 2019.

See also:

World Politics Review (August 2018) [How Facebook Made it Easier than ever to Traffic Middle Eastern Antiquities](#)
<https://conflictantiquities.wordpress.com/cv/>

Wildlife Crime

Dr. David Roberts and Julio Hernandez-Castro, "[Bycatch and illegal wildlife trade on the dark web](#)," Published online by Cambridge University Press: 14 June 2017.

National Whistleblower's Center, "[Help Stop Wildlife Trafficking on Facebook](#)," April 2018.

See also: WIRED (June 2018): [How Facebook Groups Became a Bizarre Bazaar for Elephant Tusks](#)

Bloomberg (July 2019): [A black market in wildlife trafficking thrives on Facebook and Instagram](#)

Human Remains

Dr. Shawn Graham and Dr. Damien Huffer, "[The Insta-Dead: The rhetoric of the human remains trade on Instagram](#)," *Internet Archaeology* 45, 2018.

See also: Vice (July 2018): [These Popular Instagram Accounts Are Selling Human Remains](#)

Media and Other Published Reports

Narcotics:



Ahmed Al-Rawi, "[The fentanyl crisis & the dark side of social media](#)," School of Communication, Faculty of Communication, Art and Technology, Simon Fraser University, 8888 University Drive, British Columbia V5A 1S6, Canada

Sarah Frier, "[Facebook's Crisis Management Algorithm Runs on Outrage](#)," Bloomberg, March 2019.

Romance Scams

Jack Nicas, "[Facebook Connected Her to a Tattooed Soldier in Iraq. Or So She Thought.](#)" New York Times, 28 July 2019.

Child Abuse

Michael Keller and Gabriel Dance, "[The Internet Is Overrun with Images of Child Sexual Abuse. What Went Wrong?](#)"

Mr. DOYLE. The gentlelady yields back.

Ms. Oyama, you are recognized for 5 minutes.

STATEMENT OF KATHERINE OYAMA

Ms. OYAMA. Chairman Doyle, Chairwoman Schakowsky, Ranking Members Latta and McMorris Rodgers, distinguished members of the committee, thank you for the opportunity to appear before you today. I appreciate your leadership on these important issues and welcome the opportunity to discuss Google's work in these areas.

My name is Katie Oyama, and I am the global head of IP policy at Google. In that capacity, I also advise the company on public policy frameworks for the management and moderation of online content of all kinds.

At Google, our mission is to organize and make the world's information universally accessible and useful. Our services and many others are positive forces for creativity, learning, and access to information.

This creativity and innovation continues to yield enormous economic benefits for the United States. However, like all means of communications that came before it, the internet has been used for both the best and worst of purposes. And this is why, in addition to respecting local law, we have robust policies, procedures, and community guidelines that govern what activity is permissible on our platforms, and we update them regularly to meet the changing needs of both our users and society.

In my testimony today, I will focus on three areas: the history of 230 and how it has helped the internet grow; how 230 contributes to our efforts to take down harmful content; and Google's policies across our products.

Section 230 of the Communications Decency Act has created a robust internet ecosystem where commerce, innovation, and free expression thrive, while also enabling providers to take aggressive steps to fight online abuse. Digital platforms help millions of consumers find legitimate content across the internet, facilitating almost \$29 trillion in online commerce each year.

Addressing illegal content is a shared responsibility, and our ability to take action on problematic content is underpinned by 230. The law not only clarifies when services can be held liable for third-party content, but also creates the legal certainty necessary for services to take swift action against harmful content of all types.

Section 230's Good Samaritan provision was specifically introduced to incentivize self-monitoring and to facilitate content moderation. It also does nothing to alter platform liability for violations of Federal criminal laws, which are expressly exempted from the scope of the CDA.

Over the years, the importance of Section 230 has only grown and is critical in ensuring continued economic growth. A recent study found that over the next decade, 230 will contribute an additional 4.25 million jobs and \$440 billion in growth to the economy.

Furthermore, investors in the startup ecosystem have said that weakening online safe harbors would have a recessionlike impact on investment. And internationally, 230 is a differentiator for the U.S. China, Russia, and others take a very different approach to

innovation and to censoring speech online, sometimes including speech that is critical of political leaders.

Perhaps the best way to understand the importance of 230 is to imagine what might happen if it weren't in place. Without 230, search engines, video sharing platforms, political blogs, startups, review sites of all kinds would either not be able to moderate content at all, or they would overblock, either way harming consumers and businesses that rely on their services every day.

Without 230, platforms could be sued for decisions around removal of content from their platforms, such as the removal of hate speech, mature content, or videos relating to pyramid schemes.

And because of 230, we can and do enforce rigorous policies that ensure that our platforms are safe, useful, and vibrant for our users. For each product, we have a specific set of rules and guidelines that are suitable for the type of platform, how it is used, and the risk of harm associated with it. These approaches range from clear content policies and community guidelines with flagging mechanisms to report content that violates them to increasingly effective machine learning that can facilitate removal of harmful content at scale before a single human user has ever been able to access it.

For example, in the 3-month period from April to June 2019, YouTube removed over 9 million videos from our platform for violating our community guidelines, and 87 percent of this content was flagged by machines first rather than by humans. And of those detected by machines, 81 percent of that content was never viewed by a single user.

We now have over 10,000 people across Google working on content moderation. We have invested hundreds of millions of dollars for these efforts.

In my written testimony, I go into further detail about our policies and procedures for tackling harmful content on Search, Google Ads, and YouTube.

We are committed to being responsible actors who are part of the solution. Google will continue to invest in the people and the technology to meet this challenge. We look forward to continued collaboration with the committee as it examines these issues.

Thank you for your time, and I look forward to taking your questions.

[The prepared statement of Ms. Oyama follows:]



**Written Testimony of Katherine Oyama
Global Head of Intellectual Property Policy**

**United States House of Representatives
Energy and Commerce Committee
Communications & Technology and Consumer Protection & Commerce
Subcommittees**

"Fostering a Healthier Internet to Protect Consumers"

October 16, 2019

Chairman Doyle and Chairwoman Schakowsky, Ranking Members Latta and McMorris Rodgers, and distinguished members of the Committee: Thank you for the opportunity to appear before you today. I appreciate your leadership on the important issues of consumer protection, content moderation, and free expression online, and I welcome the opportunity to discuss Google's work in these areas.

My name is Katherine Oyama, and I am the Global Head of Intellectual Property Policy at Google. In that capacity, I also advise the company on public policy frameworks for the management and moderation of online content of all kinds.

At Google, our mission is to organize the world's information and make it universally accessible and useful. We build tools that empower users to access, create, and share information like never before — giving them more choice, opportunity, and exposure to a diversity of opinions.

Our services and many others are positive forces for creativity, learning, and access to information. You can see this everyday in a variety of ways. For instance, online services have long been a place for breaking news, exposing injustices, and sharing content from places without reliable access to other forms of media. The openness of the internet has democratized how stories — and whose stories — get told, and has created a platform where anyone can succeed. Services that host original, user-generated content are stimulating an explosion of new creativity, making it easier than ever for creators of all types — amateur and professional, new and established — to find their audiences.

This creativity and innovation continues to yield enormous economic benefits for the United States. Digital platforms help millions of consumers find legitimate content across the internet, facilitating almost \$29 trillion USD in online commerce each year.¹ In 2018, the internet sector contributed \$2.1 trillion to the U.S. economy and created 6 million jobs.² Last year, Google's search and advertising tools alone helped provide \$335 billion of economic activity within the United States for more than 1.3 million businesses, website publishers, and nonprofit organizations.³

However, like all means of communications before it, the internet has been used for both the best and the worst of purposes. While educators, artists, and small businesses learned to tap into its openness in order to reach broader audiences, nefarious actors learned to use it as well for their own goals. This is why, in addition to respecting local law, we have developed robust policies, procedures, and community guidelines that govern what activity is permissible on our platforms and update them regularly to meet the changing needs of both our users and society.

¹ United Nations Conference on Trade and Development, "Global e-Commerce sales surged to \$29 trillion USD" (March 29, 2019), available at <https://unctad.org/en/pages/PressRelease.aspx?OriginalVersionID=505>.

² Internet Association, "Measuring The U.S. Internet Sector: 2019" (September 26, 2019), Available at: <https://internetassociation.org/publications/measuring-us-internet-sector-2019/>.

³ <https://economicimpact.google.com/>

Addressing illegal content is a shared responsibility, and our ability to take action on problematic content is underpinned by section 230 (“§230”) of the Communications Decency Act of 1996. The law not only clarifies where services can be held liable for third-party content, but it also creates the legal certainty necessary for services like ours to take swift action against harmful content of all types. It also does nothing to alter platform liability for violations of federal criminal laws, which are expressly exempted from the scope of the Communications Decency Act. And it makes clear that any entity that is responsible, in whole or in part, for the creation or development of information on its platform also is not immune under §230.

In my testimony today, I will focus on three key areas: (i) the history of §230 and how it has helped the internet grow; (ii) how §230 contributes to our efforts to take down harmful content; and (iii) our policies and systems at Google for tackling illegal and potentially harmful content.

§230 and the Growth of the Internet

As the Committee knows, §230 was first introduced in the 1990s as a result of a rising number of legal cases, including *Cubby, Inc. v. CompuServe Inc.*, and *Stratton Oakmont, Inc. v. Prodigy Services Co.*, which created a tenuous position for internet users and services. Courts found CompuServe not at fault for illegal user content because it had made no attempt to moderate, while holding Prodigy legally responsible after it had taken an “editorial” role in user content by moderating some of it. As a result of these cases and others, the law at that stage actually disincentivized taking action on truly harmful content online. §230 changed that calculus for platforms, incentivizing action against harmful content. The §230 “good Samaritan” provision was specifically introduced to incentivize self-monitoring and facilitate content moderation.

In the intervening years, the importance of §230 to the US economy has only grown. It has generated a robust internet ecosystem where commerce, innovation, and free expression all thrive — while at the same time enabling providers to develop content detection mechanisms and take aggressive steps to fight online abuse. §230 is a key contributor to the US's \$172 billion trade surplus in digital services.⁴ It is also critical in ensuring continued economic growth: A recent study found that over the next decade, §230 will contribute an additional 4.25 million jobs and \$440 billion in growth to the economy.⁵ Furthermore, investors in the startup ecosystem -- who drive early investment in new technologies -- have said that weakening online safe harbors would have a recession-like impact on investment.⁶ §230 is also a differentiator for the US: China, Russia, and others take a very different approach to regulating and censoring speech online, sometimes including speech that is critical of political leaders.⁷

§230 and Corporate Responsibility Online

Perhaps the best way to understand the importance of §230 is to think about what might happen if it were not in place. Without §230, platforms could face liability for decisions around removal of content from their platforms. Review sites (like Yelp, TripAdvisor, or Angie's List) might be sued for defamation claims brought by a restaurant, hotel, or an electrician trying to suppress their negative reviews.

⁴ Internet Association, "A Look At American Digital Exports" (January 23, 2019), available at: <https://internetassociation.org/publications/a-look-at-american-digital-exports/>

⁵ NetChoice and the Copia Institute, "Don't Shoot The Message Board: How Intermediary Liability Harms Online Investment and Innovation" (June 25, 2019), available at: <https://netchoice.org/report-section-230-enables-american-innovation-to-flourish-igniting-investment-opportunities-for-startups/>.

⁶ Booz & Company, Inc., "The Impact of U.S. Internet Copyright Regulations on Early-Stage Investment A Quantitative Study" (2011), available at <https://www.fifthera.com/perspectives-blog/2014/12/9/the-impact-of-internet-copyright-regulations-on-early-stage-investment>.

⁷ See: Aunpam Chander, "How Law Made Silicon Valley" (August 15, 2013), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2340197"; Adrian Shahbaz, "Freedom on the Net 2018", available at <https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism>; AccessNow and EDRI, "Content regulation – what's the (online) harm?" (October 9, 2019), available at <https://edri.org/content-regulation-whats-the-online-harm/>.

Professional and business sites, like LinkedIn and Glassdoor, might face liability if one of their users circulated a false rumor about what it's like to work at a particular company. Marketplaces like Amazon, eBay, and OfferUp might be sued for negative product reviews. Crowdfunding sites like Patreon and GoFundMe could face liability if a user posted comments about someone else that were perceived to be defamatory. Video platforms like YouTube and content-sharing apps like Instagram might face legal claims for removing videos they determined could harm or mislead users. Even email providers and search engines might be sued for trying to weed out spam and malware. Without §230, search engines, video sharing platforms, political blogs, startups, and review sites of all kinds would either not be able to filter content at all (resulting in more offensive online content, including adult content, spam, security threats, etc.) or would over-filter content (including important cases of political speech) -- in either scenario, harming consumers and businesses that rely on and use these services every day.

Because of §230, we enforce rigorous policies to ensure that our platforms are safe, useful, and vibrant for our users. It may be hard to recall the early days of the internet, when a search could yield page after page of duplicate, irrelevant content. §230 is critical to the removal of spam and malware, helping users access the information they are seeking. At Google, we have had responsible content policies in place from the early days of our company; and as time has gone by, they have evolved alongside our products.

Our Policies and Systems

Our strategy for tackling illegal and potentially harmful content is tailored to each of our platforms. For each of our products, we have a specific set of rules and guidelines that are suitable for the type of platform, how it is used, and the risk of harm associated with it. These approaches range from clear policies and community guidelines, with mechanisms to report content that violates them, to increasingly

effective artificial intelligence (AI) and machine learning that can facilitate removal of harmful content before a single human user has been able to access it. We also now have over 10,000 people across Google working on content moderation and removal on our platforms and have invested hundreds of millions of dollars in these efforts.

YouTube

Around 2 billion people come to YouTube every month and over 500 hours of video are uploaded every minute — making it one of the largest living collections of cultural content ever assembled in one place. The vast majority of this content is positive, ranging from “how-to” tutorials, family videos, journalism, and entertainment to educational and artistic content and more. In fact, over a billion educational videos are viewed on YouTube each day. At the same time, YouTube continues to drive revenue to creators on the platform. YouTube channels making over six figures in revenue are up 40 percent over the last year. And in the last 12 months alone, we’ve paid out over \$3 billion to the music industry.

While problematic or borderline content on YouTube accounts for less than 1% of the content on the platform, we are constantly working to draw effective, appropriate lines. Deciding what content is allowed on our platforms, while preserving people’s right to express themselves, is a big responsibility. It means developing rules that we can enforce consistently. It means balancing respect for diverse viewpoints and giving a platform to marginalized voices, while developing thoughtful policies to tackle egregious content that violates our rules. Over the years, we have developed a variety of tools in response to content challenges. On YouTube, we remove content that violates our policies, elevate authoritative content, reduce the spread of borderline content, and reward trusted creators.

YouTube's Community Guidelines provide clear rules of the road for what content we do and do not allow.⁸ We police content that violates these guidelines in two key ways: (1) a thorough review system that combines the efforts of machines and humans to enforce our policies; and (2) the support of our community members who flag content that violates our guidelines. As a result, videos that violate our policies generate a fraction of a percent of the views on YouTube.

We use a mix of machines and people to enforce our policies at scale. Machine learning is allowing us to identify and remove violative content faster than ever before. And our investment in technology enables us to address enforcement of our content policies at scale. Machines flag suspect videos for review by trained teams, who can analyze the content and take quick action. This system has had a major impact on the way we tackle harmful content, and has helped our human reviewers remove content more quickly.

The statistics show that our machine learning tools are able to remove violative content at scale. Between April and June 2019, YouTube removed over 9 million videos for violating our community guidelines.⁹ Over 87% of these were first flagged by machines rather than humans. Of those detected by machines, 81% were never viewed. YouTube also removed over 537 million comments that violated our community guidelines, 99% of which were detected by our automated flagging systems. This accounts for only a fraction of the billions of comments posted on YouTube each quarter.

As mentioned earlier, we have a "flagging" system through which our user community helps enforce our policies by notifying us of any content that violates our guidelines. The option to report or "flag" content that breaches our community guidelines is available under every YouTube video and comment, and we receive flags from an

⁸ <https://www.youtube.com/about/policies/#community-guidelines>

⁹ <https://transparencyreport.google.com/youtube-policy/removals?hl=en>.

engaged and diverse global community. Along with providing YouTube users with a means to flag content, we have built a network of what we call “Trusted Flaggers”. These are experts, often associated with non-governmental or specialist organizations, who have a high accuracy rate in identifying videos that might violate our guidelines. Between April and June 2019, we removed 1,152,263 videos thanks to Trusted Flaggers and users, which helped us to identify and take action against content that does not meet our community guidelines.

Our efforts do not end there, as we are constantly adapting to new challenges and looking for ways to improve our policies. We work closely with experts on an ongoing basis as we review our policies and, in 2018 alone, we made more than 30 updates. For example, in June 2019 we updated our existing community guidelines for hate speech to make it clear that our rules specifically prohibit videos alleging that one group of people is superior in order to justify discrimination, segregation, or exclusion based on qualities like age, gender, race, caste, religion, sexual orientation, or veteran status.¹⁰ In addition, our guidelines now make it crystal clear that we will remove content denying that well-documented violent events took place, like the Holocaust. These changes to our approach toward hateful content were developed in consultation with dozens of experts in subjects like violent extremism, supremacism, civil rights, and free speech.

Search and Google Ads

Google Search is a web search engine that indexes hundreds of billions of webpages. That index is well over 100 billion gigabytes in size. We do not host the content in Search and cannot influence its mere presence online, so we take different approaches to keeping people safe when using the product, including the use of ranking algorithms to surface relevant and high quality information. We also take measures to prevent poor quality or harmful content from rising in search results.

¹⁰ <https://youtube.googleblog.com/2019/06/our-ongoing-work-to-tackle-hate.html>

When it comes to removing web pages from Google Search, we are strongly guided by local law and decisions from the courts. This includes removing child sexual abuse material, copyright infringing material, and other illegal content. Our approach is based on the belief that, when it comes to questions about what information should be stripped from public availability, those lines are better drawn by lawmakers than by Google. That being said, there are some narrow circumstances¹¹ in which we may remove links from organic listings, including when we identify violations of our guidelines¹² — for example, sites with deceptive or manipulative behavior designed to deceive our users. Google suppresses or demotes approximately 19 billion web spam impressions from Search results every day.

While we need to prevent bad actors from gaming our systems through manipulation, spam, fraud, or other forms of abuse, we understand that transparency is crucial to maintaining user trust. So in addition to publishing our Search Quality Rater Guidelines, we provide information about Search on our “How Search Works” site.¹³ We also publish an annual Transparency Report,¹⁴ sharing data on how government actions and policies affect privacy, security, and access to information online. The Transparency Report provides users with detailed information on removals to ensure they understand how and why Google removes content from its platforms.

Finally, in order to protect users and enable a safe advertising ecosystem, we have strict policies across our advertising products and enforce them using both automated and human evaluation.¹⁵ In 2018 we took down 2.3 billion ads for violating our policies.¹⁶ That’s more than six million bad ads every day, and we’re able to

¹¹ <https://www.google.com/search/howsearchworks/mission/open-web/>

¹² <https://support.google.com/webmasters/answer/35769?hl=en>

¹³ <https://www.google.com/search/howsearchworks/>

¹⁴ <https://transparencyreport.google.com/>

¹⁵ <https://support.google.com/adspolicy/answer/6008942?hl=en>

¹⁶ <https://www.blog.google/products/ads/enabling-safe-digital-advertising-ecosystem/>

prevent the majority of fraud and policy violations before ads are ever even shown. This includes ads removed from approximately 1.2 million pages, more than 22,000 apps, and nearly 15,000 sites across our ad network for violations of policies directed at misrepresentative, hateful, or other low-quality content. Using improved machine learning technology, we were able to identify and terminate almost one million bad advertiser accounts, nearly double the amount we terminated in 2017.

Conclusion

We take the safety of our users very seriously and value our close and collaborative relationships with law enforcement, government agencies, and policymakers. We understand that these are difficult issues of great interest to Congress and want to be responsible actors who are a part of the solution. As these issues evolve, Google will continue to invest in the people and technology to meet the challenges at hand. We look forward to continued collaboration with the Committee as it examines these issues. Thank you for your time. I look forward to taking your questions.

Mr. DOYLE. Thank you.
Dr. Farid, you have 5 minutes.

STATEMENT OF HANY FARID, PH.D.

Dr. FARID. Chairman, Chairwoman, ranking members, members of both subcommittees, thank you for the opportunity to speak with you today.

Technology, as you have already heard, and the internet have had a remarkable impact on our lives and society. Many educational, entertaining, and inspiring things have emerged from the past two decades in innovation.

But at the same time, many horrific things have emerged: a massive proliferation of child sexual abuse material; the recruitment and radicalization of domestic and international terrorists; the distribution of illegal and deadly drugs; the proliferation of mis- and disinformation campaigns designed to sow civil unrest, incite violence, and disrupt democratic elections; the proliferation of dangerous, hateful, and deadly conspiracy theories; the routine and daily harassment of women and underrepresented groups in the forms of threats of sexual violence and revenge and nonconsensual pornography; small and large-scale fraud; and spectacular failures to protect our personal and sensitive data.

How in 20 short years did we go from the promise of the internet to democratize access to knowledge and make the world more understanding and enlightened to this litany of daily horrors? A combination of naivete, ideology, willful ignorance, and a mentality of growth at all costs have led the titans of tech to fail to install proper safeguards on their services.

The problem that we face today, however, is not new. As early as 2003, it was well known that the internet was a boon for child predators. Despite early warnings, the technology sector dragged their feet through the early and mid-2000s and did not respond to the known problems at the time, nor did they put in place the proper safeguards to contend with what should have been the anticipated problems that we face today.

In defense of the technology sector, they are contending with an unprecedented amount of data. Some 500 hours of video are uploaded to YouTube every minute, some 1 billion daily uploads to Facebook, and some 500 million tweets per day.

On the other hand, these same companies have had over a decade to get their houses in order and have simply failed to do so. And at the same time, they have managed to profit handsomely by harnessing the scale and volume of the data that is uploaded to their services every day.

And these services don't seem to have trouble dealing with unwanted material when it serves their interests. They routinely and quite effectively remove copyright infringement, and they effectively remove legal adult pornography because otherwise, their services would be littered with pornography, scaring away advertisers.

During his 2018 congressional testimony, Mr. Zuckerberg repeatedly invoked artificial intelligence, AI, as the savior for content moderation in, we are told, 5 to 10 years. Putting aside that it is

not clear what we should do in the intervening decade or so, this claim is almost certainly overly optimistic.

So, for example, earlier this year, Facebook's chief technology officer showcased Facebook's latest AI technology for discriminating images of broccoli from images of marijuana. Despite all of the latest advances in AI and pattern recognition, this system is only able to perform the task with an average accuracy of 91 percent. This means that approximately 1 in 10 times, the system is simply wrong.

At a scale of a billion uploads a day, this technology cannot possibly automatically moderate content. And this discrimination task is surely much easier than the task of identifying a broad class of child exploitation, extremism, and disinformation material.

The promise of AI is just that, a promise, and we cannot wait a decade or more with the hope that AI will improve by some nine orders of magnitude when it might be able to contend with automatic online content moderation.

To complicate things even more, earlier this year Mr. Zuckerberg announced that Facebook is implementing end-to-end encryption on its services, preventing anyone—the government, Facebook—from seeing the contents of any communications. Blindly implementing end-to-end encryption will make it even more difficult to contend with the litany of abuses that I enumerated at the opening of my remarks.

We can and we must do better when it comes to contending with some of the most violent, harmful, dangerous, and hateful content online. I simply reject the naysayers that argue that it is too difficult from a policy or technological perspective or those that say that reasonable and responsible content moderation will lead to the stifling of an open exchange of ideas.

Thank you, and I look forward to taking your questions.

[The prepared statement of Dr. Farid follows:]

House Committee on Energy and Commerce
Fostering a Healthier Internet to Protect Consumers

Hany Farid, Ph.D.

Testimony

Background

Technology and the internet have had a remarkable impact on our lives and society. Many educational, entertaining, and inspiring things have emerged from the past two decades in innovation. At the same time, many horrific things have emerged: a massive proliferation of child sexual abuse material [5], the spread and radicalization of domestic and international terrorists [2], the distribution of illegal and deadly drugs [10], the proliferation of mis- and dis-information campaigns designed to sow civil unrest, incite violence, and disrupt democratic elections [1], the proliferation of dangerous, hateful, and deadly conspiracy theories [9], the routine harassment of women and under-represented groups in the form of threats of sexual violence and revenge and non-consensual pornography [3], small- to large-scale fraud [12], and spectacular failures to protect our personal and sensitive data [4].

How, in 20 short years, did we go from the promise of the internet to democratize access to knowledge and make the world more understanding and enlightened, to this litany of daily horrors? Due to a combination of naivete, ideology, willful ignorance, and a mentality of growth at all costs, the titans of tech have simply failed to install proper safeguards on their services.

The Past

The landmark case of *New York v. Ferber* made it illegal to create, distribute, or possess child sexual abuse material (CSAM). The result of this ruling, along with significant law enforcement efforts, was effective, and by the mid-1990s, CSAM was, according to the National Center for Missing and Exploited Children on the way to becoming a “solved problem.” By the early 2000s, however, the rise of the internet brought with it an explosion in the global distribution of CSAM. Alarmed by this growth, in 2003, Attorney General Ashcroft convened executives from the top technology firms to ask them to propose a solution to eliminate this harmful content from their networks. Between 2003 and 2008 these technology companies did nothing to address the ever-growing problem of their online services being used to distribute a staggering amount of CSAM with increasingly violent acts on increasingly younger children (as young, in some cases, as a only a few months old).

In 2008, Microsoft invited me to attend a yearly meeting of a dozen or so technology companies to provide insight into why, after five years, there was no solution to the growing and troubling spread of CSAM online. Convinced that a solution was possible, I began a collaboration with Microsoft researchers to develop technology that could quickly and reliably identify and remove CSAM from online services. Within a year we had developed and deployed such a technology –

photoDNA, a robust hashing technology¹. PhotoDNA has, in the intervening decade, seen global adoption (it is licensed at no cost) and has proven to be effective in disrupting the global distribution of previously identified CSAM: more than 95% of the nearly 18 million reports in 2018 to NCMEC's CyberTipline, constituting over 45 million pieces of identified CSAM, were from photoDNA.

This story illustrates an important point. The issue of inaction for more than five years was never one of technological limitations, it was simply an issue of will – the major technology companies at the time simply did not want to solve the problem. This is particularly inexcusable given that we were addressing some of the most unambiguously violent, heinous, and illegal content being shared on their services. The issue was, in my opinion, one of a fear. Fear that if it could be shown that CSAM could be efficiently and effectively removed, then the technology sector would have no defense for not contending with myriad abuses on their services.

The Present

In the intervening decade following the development and deployment of photoDNA, the titans of tech have barely done anything to improve or expand this technology. This is particularly stunning for an industry that prides itself on bold and rapid innovation.

In the defense of the technology sector, they are contending with an unprecedented amount of data: some 500 hours of video uploaded to YouTube every minute, some one billion daily uploads to Facebook, and some 500 million tweets per day. On the other hand, these same companies have had over a decade to get their house in order and have simply failed to do so. At the same time, they have managed to profit handsomely by harnessing the scale and volume of data uploaded to their services. And, these services don't seem to have trouble dealing with unwanted material on their services when it serves their interests. They routinely and quite effectively remove copyright infringement material (because of the Digital Millennium Copyright Act, DMCA) and adult pornography (which is a violation of, for example, Facebook's and YouTube's terms of service).

During his 2018 Congressional testimony, Mr. Zuckerberg repeatedly invoked artificial intelligence (AI) as the savior for content moderation (in 5 to 10 years time). Putting aside that it is not clear what we should do in the intervening decade, this claim is almost certainly overly optimistic.

Earlier this year, for example, Mike Schroepfer, Facebook's chief technology officer, showcased Facebook's latest AI technology for discriminating images of broccoli from images of marijuana [7]. Despite all of the latest advances in AI and pattern recognition, this system is only able to perform this task with an average accuracy of 91%. This means that approximately 1 in 10 times, the system is wrong. At the scale of a billion uploads a day, this technology cannot possibly automatically moderate content. And, this discrimination task is surely much easier than the task of identifying the broad class of CSAM, extremism, or dis-information material.

By comparison, the robust image hashing technique used by photoDNA has an expected error rate of approximately 1 in 50 billion. The promise of AI is just that, a promise, and we cannot wait a decade (or more) with the hope that AI will improve by nine orders of magnitude when it might be able to contend with automatic online content moderation.

In the meantime, AI and similar technologies can be used as a triage, reducing the amount of content that will eventually have to be viewed by human moderators. This, however, still poses considerable challenges given the woeful low number of moderators and the truly horrific working conditions that moderators are forced to endure [8].

¹Robust image hashing algorithms like photoDNA work by extracting a distinct digital signature from known harmful or illegal content and comparing these signatures against content at the point of upload. Flagged content can then be instantaneously removed and reported.

The simple fact is that the titans of tech have not invested in the infrastructure, technology, or human moderation to deal with the abuses that they know occur every day on their services. The largest point of tension is that the majority of social media is driven by advertising dollars which in turn means that they are motivated to maximize the amount of time that users spend on their services. Optimizing for the number of users and user engagement is, in many cases, at odds with effective content moderation.

End-to-End Encryption

Earlier this year, Mr. Zuckerberg announced that Facebook is implementing end-to-end encryption on its services, preventing anyone — including Facebook — from seeing the contents of any communications [14]. In announcing the decision, Mr. Zuckerberg conceded that it came at a cost:

“At the same time, there are real safety concerns to address before we can implement end-to-end encryption across all of our messaging services,” he wrote. “Encryption is a powerful tool for privacy, but that includes the privacy of people doing bad things. When billions of people use a service to connect, some of them are going to misuse it for truly terrible things like child exploitation, terrorism, and extortion.”

The adoption of end-to-end encryption would significantly hamper the efficacy of programs like photoDNA. This is particularly troubling given that the majority of the millions of yearly reports to NCMEC’s CyberTipline originate on Facebook’s Messaging services. Blindly implementing end-to-end encryption will significantly increase the risk and harm to children around the world, not to mention the inability to contend with other illegal and dangerous activities on Facebook’s services.

Many in law enforcement have made the case that a move to end-to-end encryption, without allowing access under a lawful warrant, would severely hamper law enforcement and national security efforts [13]. Programs like photoDNA, for example, would be rendered completely ineffective within an end-to-end encrypted system. In response, Attorney General Barr and his British and Australian counterparts have openly urged Mr. Zuckerberg to delay the implementation of end-to-end encryption until proper safeguards can be put in place [6], as have the 28 European Union Member States².

We should continue to have the debate between balancing privacy afforded by end-to-end encryption and the cost to our safety. In the meantime, recent advances in encryption and robust hashing technology mean that technologies like photoDNA – robust image hashing – can be adapted to operate within an end-to-end encryption system.

Specifically, when using certain types of encryption algorithms (so-called partially- or fully-homomorphic encryption), it is possible to perform the same type of robust image hashing on encrypted data [11]. This means that encrypted images can be analyzed to determine if they are known illicit or harmful material without the need, or even ability, to decrypt the image. For all other images, this analysis provides no information about its contents, thus preserving content privacy.

²The 28 EU Member States recently approved by unanimity a declaration on combating the sexual abuse of children and directly addresses this issue of end-to-end encryption writing: “Offenders make use of encryption and other anonymisation techniques to hide their identity and location. They use communication platforms hosted and administered in different countries to groom children into abuse and to extort them to obtain abusive material, as law enforcement, hampered by obfuscation techniques and different legislative regimes across different jurisdictions, especially in third countries, struggles to take forward investigations. The Council urges the industry to ensure lawful access for law enforcement and other competent authorities to digital evidence, including when encrypted or hosted on IT servers located abroad, without prohibiting or weakening encryption and in full respect of privacy and fair trial guarantees consistent with applicable law.”

Alternatively, robust image hashing can be implemented at the point of transmission, as opposed to the current approach where it is implemented upon receipt. In this client-side implementation, the distinct signature is extracted prior to encryption and transmitted alongside the encrypted message. Because no identifying information can be extracted from this signature, it does not reveal any details about the encrypted image while allowing for the monitoring of known CSAM and other harmful material.

Counter-Arguments

The argument against better content moderation and end-to-end encryption usually fall into one of several categories.

- *Freedom of expression.* It is argued that content moderation is a violation of the freedom of expression. It is not. Online services routinely ban protected speech for a variety of reasons, and can do so under their terms of service. Facebook and YouTube, for example, do not allow (legal) adult pornography on their services and do a fairly good job of removing this content. The reason they do this is because without this rule, their services would be littered with pornography, scaring away advertisers. You cannot ban protected speech and then hide behind freedom of expression as an excuse for inaction.
- *Marketplace of ideas.* It is argued that we should allow all forms of speech and then allow users to choose from the marketplace of ideas. There is, however, no counter-speech to child sexual abuse material, bomb-making and beheading videos, threats of rape, revenge porn, or fraud. And even if there was, the marketplace of ideas only works if the marketplace is fair. It is not: the online services have their thumbs on the scale because they promote content that engages users to stay on their services longer and this content tends to be the most outrageous, salacious, and controversial.
- *Sunshine.* It is argued that “sunshine is the best disinfectant,” and that the best way to counter hate-speech is with more speech. This, again, assumes a fair marketplace where ideas are given equal airtime, and that the dialogue around competing viewpoints is reasoned, thoughtful, and respectful. Perhaps this is true at the Oxford debate club, but it is certainly not the case on YouTube, Twitter, and Facebook where some of the most hateful, illegal, and dangerous content is routinely shared and celebrated. Perhaps sunshine is the best disinfectant – but for germs, not the plague.
- *Complexity.* It is argued by the technology companies that content moderation is too complex because material often falls into a gray area where it is difficult to determine its appropriateness. While it is certainly true that some material can be difficult to classify, it is also true that large amounts of material are unambiguously illegal or violations of terms of service. There is no need to be crippled by indecision when it comes to this clear-cut content.
- *Slippery slope.* It is argued that if we remove one type of material, then we will remove another, and another, and another, thus slowly eroding the global exchange of ideas. It is difficult to take this argument seriously because in the physical world we place constraints on speech without the predicted dire consequences. Why should the online world be any different when it comes to removing illegal and dangerous content?
- *Privacy.* It is argued that end-to-end encryption, without safeguards or access under a lawful warrant, is necessary to protect our privacy. Erica Portnoy, from the Electronic Frontier

Foundation (EFF), for example, argues that “A secure messenger should provide the same amount of privacy as you have in your living room. And the D.O.J. is saying it would be worth putting a camera in every living room to catch a few child predators.” [13] On the first part, we agree: you have certain expectations of privacy in your living room, but not absolute privacy. On the second part, we disagree: First, the DOJ is not asking to place a camera in every living room. It is asking to be allowed to view content when a lawful warrant has been issued, as it can in your living room. And lastly, is the EFF really comfortable referring to 45 million pieces of child sexual abuse material reported to NCMEC last year as “a few child predators?”

Conclusions

We can and we must do better when it comes to contending with some of the most violent, harmful, dangerous, and hateful content online. I reject the naysayers that argue that it is too difficult or impossible, or those that say that reasonable and responsible content moderation will lead to the stifling of an open exchange of ideas.

References

- [1] S. Bradshaw and P. Howard. The global disinformation order. *Computational Propaganda Research Project*, Sep 2019.
- [2] M. Fisher and A. Taub. How everyday social media users become real-world extremists. *New York Times*, Apr 2018.
- [3] S. Haynes. ‘A toxic place for women.’ a new study reveals the scale of abuse on Twitter. *Time*, Dec 2018.
- [4] V. Ho. Facebook’s privacy problems: a roundup. *The Guardian*, Dec 2018.
- [5] M. Keller and G. Dance. The internet is overrun with images of child sexual abuse. what went wrong? *New York Times*, Sep 2019.
- [6] R. McMillan, J. Horwitz, and D. Volz. Barr presses Facebook on encryption, setting up clash over privacy. *Wall Street Journal*, Oct 2019.
- [7] C. Metz and M. Isaac. Facebook’s A.I. whiz now faces the task of cleaning it up. sometimes that brings him to tears. *New York Times*, May 2019.
- [8] C. Newton. Bodies in seats. *The Verge*, Jun 2019.
- [9] B. Resnick. Social media’s conspiracy theory problem isn’t going away. *Vox*, Aug 2019.
- [10] D. Scott. This is how easy it is to order deadly opioids over the internet. *Vox*, Jan 2018.
- [11] P. Singh and H. Farid. Robust homomorphic image hashing. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 11–18, 2019.
- [12] S. Tompor. Scammers are fooling millennials out of millions of dollars: Here’s how. *Detroit Free Press*, Oct 2019.
- [13] J. Valentino-DeVries and G. Dance. Facebook encryption eyed in fight against online child sex abuse. *New York Times*, Oct 2019.
- [14] M. Zuckerberg. A privacy-focused vision for social networking, Mar 2019.

Mr. DOYLE. Thank you, Dr. Farid.

Well, we have concluded our openings. We are going to move to Member questions. Each Member will have 5 minutes to ask questions of our witnesses, and I will start by recognizing myself for 5 minutes.

Well, I have to say, when I said at the beginning of my remarks this is a complex issue, it is a very complex issue, and I think we have all heard the problems. What we need to hear is solutions.

Let me just start by asking all of you, just by a show of hands: Who thinks that online platforms could do a better job of moderating their content on their websites?

So that is unanimous, and I agree. And I think it is important to note that we all recognize that content moderation online is lacking in a number of ways and that we all need to address this issue better. And if not you, who are the platforms and the experts in this technology, and you put that on our shoulders, you may see a law that you don't like very much and that has a lot of unintended consequences for the internet.

So I would say to all of you, you need to do a better job. You need to have an industry getting together and discussing better ways to do this. The idea that you can buy drugs online and we can't stop that, to most Americans hearing that, they don't understand why that is possible, why it wouldn't be easy to identify people that are trying to sell illegal things online and take those sites down. Child abuse. It is very troubling.

On the other hand, I don't think anybody on this panel is talking about eliminating Section 230. So the question is, what is the solution between not eliminating 230, because of the effects that would have just on the whole internet, and making sure that we do a better job of policing this?

Mr. Huffman, Reddit, a lot of people know of Reddit, but it is really a relatively small company when you place it against some of the giants. And you host many communities, and you rely on your volunteers to moderate discussions. I know that you have shut down a number of controversial sub-Reddits that have spread deepfakes, violent and disturbing content, misinformation, and dangerous conspiracy theories. But what would Reddit look like if you were legally liable for the content your users posted or for your company's decision to moderate user content and communities?

Mr. HUFFMAN. Sure. Thank you for the question.

What Reddit would look like would be—we would be forced to go to one of two extremes. In one version, we would stop looking. We would go back to the pre-230 era, which means if we don't know, we are not liable. And that, I am sure, is not what you intend, and it is certainly not what we want. It would be not aligned with our mission of bringing community and belonging to everybody in the world.

The other extreme would be to remove any content or prohibit any content that could be remotely problematic. And since Reddit is a platform where 100 percent of our content is created by our users, it fundamentally undermines the way Reddit works. It is hard for me to give you an honest answer of what Reddit would look like, because I am not sure Reddit, as we know it, could exist in a world where we had to remove all user-generated content.

Mr. DOYLE. Yes.

Dr. McSherry, you talk about the risk to free speech if Section 230 were repealed or substantially altered, but what other tools could Congress use to incentivize online platforms to moderate dangerous content and encourage a healthier online ecosystem? What would your recommendation be short of eliminating 230?

Dr. MCSHERRY. Well, I think a number of the problems that we have talked about today so far—which I think everyone agrees are very, very serious, and I want to underscore that—are actually often addressed by existing laws that target the conduct itself. So, for example, in the Armslist case, we had a situation where what Armslist—the selling of the gun that was so controversial was actually perfectly legal under Wisconsin law.

Similarly, many of the problems that we have talked about today are already addressed by Federal criminal laws that already exist, and so they aren't—Section 230 is not a barrier, because, of course, there is a carveout for Federal criminal laws.

So I would urge this committee to look carefully at the laws that actually target the actual behavior that we are concerned about and perhaps start there.

Mr. DOYLE. Ms. Peters, you did a good job horrifying us with your testimony. What solution do you offer short of repealing 230?

Ms. PETERS. I don't propose repealing 230. I think that we want to continue to encourage innovation in this country. It is our core economic—a core driver of our economy. But I do believe that CDA 230 should be revised so that, if something is illegal in real life, it is illegal to host it online. I don't think that that is an unfair burden for tech firms. Certainly some of the wealthiest firms in our country should be able to take that on.

I, myself, have a small business. We have to run checks to make sure when we do business with foreigners that we are not doing business with somebody that is on a terror blacklist. Is it so difficult for companies like Google and Reddit to make sure that they are not hosting an illegal pharmacy?

Mr. DOYLE. I see my time is getting way expired, but I thank you, and I think we get the gist of your answer.

The chairman now yields to my ranking member for 5 minutes.

Mr. LATTA. Well, thank you, Mr. Chairman.

And again, thanks to our witnesses.

Ms. Oyama, if I could start with you. A recent New York Times article outlined the horrendous nature of child sex abuse online and how it has exponentially grown over the last decade. My understanding is tech companies are only legally required to report images of child abuse only when they discover it. They are not required to actively look for it.

While I understand you make voluntary efforts to look for this type content, how can we encourage platforms to better enforce their terms of service or proactively use their sword provided by subsection (c)(2) of Section 230 to take good faith efforts to create accountability within the platforms?

Ms. OYAMA. Thank you for the question and particularly for focusing on the importance of section (c)(2) to incentivize platforms to moderate content.

I can say that, for Google, we do think that transparency is critically important, and so we publish our guidelines, we publish our policies, we publish on YouTube a quarterly transparency report where we show across the different categories of content what is the volume of content that we have been removing.

And we also allow for users to appeal. So if their content is stricken and they think that was a mistake, they also have the ability to appeal and track what is happening with the appeal.

So we do understand that this piece of transparency is really critical to user trust and for discussions with policymakers on these critically important topics.

Mr. Latta. Thank you.

Ms. Citron, a number of defendants have claimed Section 230 immunity in the courts, some of which are tech platforms that may not use any user-generated content at all. Was Section 230 intended to capture those platforms?

Ms. Citron. So platforms are solely responsible for the content. The question is, there is no user-generated content, and they are creating the content? That is the question, would that be covered by the legal shield of 230? I am asking, is that the question?

Mr. Latta. Right.

Ms. Citron. No. They would be responsible for the content that they have created and developed. So Section 230, that legal shield, would not apply.

Mr. Latta. Thank you.

Mr. Farid, are there tools available, like PhotoDNA or Copyright ID, to flag the sale of illegal drugs online? If the idea is that platforms should be incentivized to actively scan their platforms and take down blatantly illegal content, shouldn't key words or other indicators associated with opioids be searchable through an automated process?

Dr. Farid. The short answer is yes.

There are two ways of doing content moderation. Once material has been identified, typically by a human moderator, whether that is child abuse material, illegal drugs, terrorism-related material, whatever it is, that material, copyright infringement, can be fingerprinted, digitally fingerprinted, and then stopped from future upload and distribution.

That technology has been well understood and has been deployed for over a decade. I think it has been deployed anemically across the platforms and not nearly aggressively enough. That is one form of content moderation that works today.

The second form of content moderation is what I call the day zero, finding the Christchurch video on upload. That is incredibly difficult and still requires law enforcement, journalists, or the platforms themselves to find. But once that content has been identified, it can be removed from future uploads.

And I will point out, by the way, that today you can go onto Google and you can type "buy fentanyl online" and it will show you in the first page illegal pharmacies where you can click and purchase fentanyl.

That is not a difficult find. We are not talking about the dark web. We are not talking about things buried on page 20. It is on the first page. And in my opinion, there is no excuse for that.

Mr. LATTA. Let me follow up, because you said it is anemic, what some of the platforms might be doing out there.

You know, last year in this room, we passed over 60 pieces of legislation dealing with the drug crisis that we have in this country, fentanyl being one of them. You just mentioned that you can just type in “fentanyl” and you can find it. OK. Because again, what we are trying to do is make sure we don’t have the 72,000 deaths that we had in this country over a year ago and with over 43,000 being associated with fentanyl.

So how do we go into the platforms and say, “We have got to enforce this because we don’t want the stuff flowing in from China”? And how do we do that?

Dr. FARID. Well, this is what the conversation is. So I am with everybody else on the panel, we don’t repeal 230, but we make it a responsibility, not a right. If your platform can be weaponized in the way that we have seen across the boards from the litany of things that I had in my opening remarks, surely something is not working.

If I can find on Google in page 1—and not just me, my colleagues on the table, also investigative journalists—we know this content is there. It is not hiding. It is not difficult. And we have to ask the question that, if a reasonable person can find this content, surely Google with its resources can find it as well, and now what is the responsibility?

And I think you said earlier, too, is that you just enforce your terms of service. So if we don’t want to talk about 230, let’s talk about terms of service. The terms of service of most of the major platforms are actually pretty good. It is just that they don’t really do very much to enforce them in a clear, consistent, and transparent way.

Mr. LATTA. Thank you very much.

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

Mr. DOYLE. The gentleman yields back.

The Chair now recognizes Ms. Schakowsky, chair for the Subcommittee on Consumer Protection, for 5 minutes.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

Ms. Oyama, you said in one of the sentences that you presented to us that without 230. I want to see if there are any hands that would go up, that we should abandon 230. Has anybody said that? OK.

So this is not the issue. This is a sensible conversation about how to make it better.

Mr. Huffman, you said—and I want to thank you for—we had, I think, a really productive meeting yesterday—explaining to me what your organization does and how it is unique. But you also said in your testimony that Section 230 is a unique American law. And so—but, yes. When we talked yesterday, you thought it was a good idea to put it into a trade agreement dealing with Mexico and Canada.

If it is a unique American law, let me just say that I think trying to fit it into the regulatory structure of other countries at this time is inappropriate.

And I would like to just quote, I don’t know if he is here, from a letter that both Chairman Pallone and Ranking Member Walden

wrote some time ago to Mr. Lighthizer that said, “We find it inappropriate for the United States to export language mirroring Section 230 while such serious policy discussions are ongoing.” And that is what is happening right now. We are having a serious policy discussion.

But I think what the chairman was trying to do and what I want to do is try to figure out, what do we really want to do to amend or change in some way? And so again, briefly, if the three of you that have talked about the need for changes, let me start with Ms. Citron, on what you want to see in 230.

Ms. CITRON. So I would like to bring the statute back to its original purpose, was to apply to Good Samaritans who are engaged in responsible and reasonable content moderation practices. And I have the language to change the statute that would condition that we are not going to treat a provider or user of an interactive service that engages in reasonable content moderation practices as a publisher or a speaker. So it would keep the immunity, but it would—

Ms. SCHAKOWSKY. Let me just suggest that if there is language, I think we would like to see suggestions.

Ms. Peters, if you could, and I think you pretty much scared us as to what is happening, and then how we can make 230 responsive to those concerns.

Ms. PETERS. Thank you for your question, Chair Schakowsky.

We would love to share some proposed language with you about how to reform 230 to protect better against organized crime and terror activity on platforms.

One of the things I am concerned about that a lot of tech firms are involved in is, when they detect illicit activity or it gets flagged to them by users, their response is to delete it and forget about it. What I am concerned about is two things.

Number one, that essentially is destroying critical evidence of a crime. It is actually helping criminals to cover their tracks, as opposed to a situation like what we have for the financial industry and even aspects of the transport industry. If they know that illicit activity is going on, they have to share it with law enforcement and they have to do it in a certain timeframe.

I certainly want to see the content removed, but I don’t want to see it simply deleted, and I think that is an important distinction. I would like to see a world where the big tech firms work collaboratively with civil society and with law enforcement to root out some of these evil entities.

Ms. SCHAKOWSKY. I am going to cut you off just because my time is running out and I do want to get to Dr. Farid with the same thing. So we would welcome concrete suggestions.

Dr. FARID. Thank you.

I agree with my colleague, Professor Citron. I think 230 should be a privilege, not a right. You have to show that you are doing reasonable content moderation.

I think we should be worried about the small startups. If we start regulating now, the ecosystem will become even more monopolistic. So we have to think about how do we make carveouts for small platforms who can now compete where these companies did not have to deal with that regulatory pressure.

And the last thing I will say is the rules have to be clear, consistent, and transparent.

Ms. SCHAKOWSKY. Thank you. I yield back.

Mr. DOYLE. The Chair now recognizes Mrs. McMorris Rodgers for 5 minutes.

Mrs. RODGERS. Thank you, Mr. Chairman.

Section 230 was intended to provide online platforms with a shield from liability as well as a sword to make good faith efforts to filter, block, or otherwise address certain offensive content online.

Professor Citron, do you believe companies are using the sword enough, and if not, why do you think that is?

Ms. CITRON. We are seeing the dominant platforms—I have been working with Facebook and Twitter for about 8 years—and so I would say the dominant platforms and folks on this panel at this point are engaging in what I would describe at a broad level as fairly reasonable content moderation practices.

I think they could do far better on transparency about what they mean by when they forbid hate speech. What do they mean by that? What is the harm that they want to avoid? Examples. And they could be more transparent about the processes that they use when they make decisions, right, to have more accountability.

But what really worries me are the sort of renegade sites as well, the 8chans, who foment incitement with no moderation, dating apps that have no ability to ban impersonators and have IP addresses. And frankly, sometimes, it is the biggest of providers, not the small ones, who know they have illegality happening on their platforms and do nothing about it.

Mrs. RODGERS. And why are they doing that?

Ms. CITRON. Because of Section 230 immunity. So the dating app Grindr comes to mind, hosting impersonations of someone's ex. And the person was using Grindr to send thousands of men to this man's home. Grindr heard 50 times from the individual who was being targeted, did nothing about it.

Finally, when they responded after getting a lawsuit, their response was, "Our technology doesn't allow us to track IP addresses."

But Grindr is fairly dominant in this space. But when the person went to SCRUFF, it is a smaller dating site, the impersonator was again posing as the individual, sending men to his home, and SCRUFF responded right away. They said, "We can ban the IP address" and took care of it.

So I think the notion that the smaller versus large, by my lights, is there are good practices, responsible practices, and irresponsible, harmful practices.

Mrs. RODGERS. OK. Thank you for that.

Mr. Huffman and Ms. Oyama, your company policies specifically prohibit illegal content or activities on your platform. Regarding your terms of service, how do you monitor content on your platform to ensure that it does not violate your policies?

Maybe I will start with Mr. Huffman.

Mr. HUFFMAN. Sure. So, in my opening statement, I described the three layers of moderation that we have on Reddit, our com-

pany's moderation and our team. This is the group that both writes the policies and enforces the policies.

Primarily the way they work is enforcing these policies at scale, so looking for aberrational behavior, looking for known problematic sites or words. We participate in the cross-industry hash sharing, which allows us to find images, for example, exploitive of children that are shared industrywide, or fingerprints thereof.

Next, though, are our community moderators. These are the people who—these are users—and then following the users themselves, those two groups participate together in removing content that is inappropriate for their community and in violation of our policies.

We have policies against hosting. Our content policy is not very long, but one of the points is no illegal content. So no regulated goods, no drugs, no guns, anything of that sort, controlled—

Mrs. ROGERS. So you are seeking it out, and if you find it, then you get it off the platform.

Mr. HUFFMAN. That is right, because 230 doesn't provide us criminal liability protection. And so we are not in the business of committing crimes or helping people commit crimes. That would be problematic for our business. So we do our best to make sure it is not on the platform.

Mrs. ROGERS. Thank you.

Ms. Oyama, would you address that, and then just what you are doing if you find that illegal content?

Ms. OYAMA. Thank you. Yes.

Across YouTube, we have very clear content policies. We publish those online. We have YouTube videos that give more examples and some specific ways so people understand.

We are able to detect, of the 9 million videos that we removed from YouTube in the last quarter, 87 percent of those were detected first by machine. So automation is one very important way.

And then the second way is human reviewers. So we have community flagging where any user that sees problematic content can flag it and follow what happens with that complaint. We also have human reviewers that look, and then we are very transparent in explaining that.

When it comes to criminal activity on the internet, you know, of course, CDA 230 has a complete carveout. So in the case of Grindr we have policies against harassment. But in the case of Grindr where there was real criminal activity, my understanding is there is a defendant in that case, and there is a criminal case for harassment and stalking that are proceeding against him.

And so in certain cases, opioids—again, controlled substance—under criminal law there is a section that says, I think, controlled substances on the internet, sale of controlled substances on the internet, that is a provision.

In cases like that where there is actually a law enforcement rule, we would, you know, if there is correct legal process, then we would work with law enforcement to also provide information under due process or a subpoena.

Mrs. ROGERS. Thank you.

OK. My time has expired. I yield back.

Mr. DOYLE. The gentlelady yields. Thank you.

Ms. DeGette, you are recognized for 5 minutes.

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

I really want to thank this panel. I am a former constitutional lawyer, so I am always interested in the intersection between criminality and free speech.

And in particular, Professor Citron, I was reading your written testimony, which you confirmed with Ms. Schakowsky, about how Section 230 should be revised to both continue to provide First Amendment protections but also return the statute to its original purpose, which is to let companies act more responsibly, not less.

And, in that vein, I want to talk during my line of questioning about online harassment, because this is a real—sexual harassment—this is a real issue that has just only increased. The Anti-Defamation League reported that 24 percent of women and 63 percent of LGBTQ individuals have experienced online harassment because of their gender or sexual orientation, and this is compared to only 14 percent of men, and 37 percent of all Americans of any background have experienced severe online harassment, which includes sexual harassment, stalking, physical threats, and sustained harassment.

So I want to ask you, Professor Citron, and also I want to ask you, Ms. Peters, very briefly to talk to me about how Section 230 facilitates illegal activities, and do you think it undermines the value of those laws, and if so, how.

Professor Citron.

Ms. CITRON. So let me say that in cases involving harassment, of course, there is a perpetrator and then the platform that enables it. And most of the time the perpetrators are not pursued by law enforcement. So in my book “Hate Crimes in Cyberspace” I explore the fact that law enforcement, really they don’t get the—they don’t understand the abuse, they don’t know how to investigate it.

In the case of Grindr, police—there were, like, 10 protective orders that were violated, and law enforcement in New York has done nothing about it.

So it is not true that we can always find the perpetrator, nor especially in the cases of stalking, harassment, and threats. We see a severe underenforcement of law, particularly when it comes to gendered harms.

Ms. DEGETTE. And that is really where it falls to the sites, then, to try to protect.

Ms. Peters, do you want to comment on that?

Ms. PETERS. I just wanted to say that in this issue there needs to be something akin to like a cyber restraining order, so that if somebody is stalking somebody on Grindr or OkCupid or Google, that site can be ordered to block that person from communicating with the other.

Ms. DEGETTE. OK. And even under Section 230 immunity, can platforms ignore requests to take down this type of material?

Ms. PETERS. They have.

Ms. DEGETTE. Professor Citron, you are nodding your head.

Ms. CITRON. They do and they can, especially if those protective orders are coming from State criminal law.

Ms. DEGETTE. OK.

I wanted to ask you, Dr. McSherry, sexual harassment continues to be a significant problem on Twitter and other social platforms, and I know Section 230 is a critical tool that facilitates content moderation. But, as we have heard in the testimony, a lot of the platforms aren't being aggressive enough to enforce the terms and conditions. So what I want to ask you is, what can we do to encourage platforms to be more aggressive in protecting consumers and addressing issues like harassment?

Dr. MCSHERRY. I imagine this hearing will encourage many of them to do just that.

Ms. DEGETTE. But we keep having hearings—

Dr. MCSHERRY. No, no, no. I understand. Absolutely. I understand that.

So I actually think that many, many of the platforms are pretty aggressive already in their content moderation policies. I agree with what many have said here today, which is that it would be nice if they would start by clearly enforcing their actual terms of service, which we share a concern about because often they are enforced very inconsistently, and that is very challenging for users.

A concern that I have is, if we institute what I think is one proposal, which is that whenever you get a notice you have some duty to investigate, that could actually backfire for marginalized communities, because one of the things that also happens is if you want to silence someone online, one thing you might do is flood a service provider with complaints about them. And then they end up being the ones who are silenced rather than the other way around.

Ms. DEGETTE. Dr. Farid, what is your view of that?

Dr. FARID. Pardon me?

Ms. DEGETTE. What is your view of what Dr. McSherry said?

Dr. FARID. There are two issues at hand here. When you do moderation, you risk overmoderating or undermoderating.

Ms. DEGETTE. Right.

Dr. FARID. What I would argue is we are way, way undermoderating. When I look at where we fall down and where we make mistakes and take down content we should, and I weigh that against 45 million pieces of content just last year to NCMEC and child abuse material and terrorism and drugs, the weights are imbalanced. We have to sort of rebalance, and we have to try to get it right.

We are going to make mistakes, but we are making way more mistakes on allowing content right now than we are on not allowing.

Ms. DEGETTE. Thank you.

Thank you very much, Mr. Chairman. I yield back.

Mr. DOYLE. The gentlelady yields back.

The Chair now recognizes Mr. Johnson for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman, to you and to Chairwoman Schakowsky, for holding this very important hearing.

You know, I have been in information technology for most of my adult life, and social responsibility has been an issue that I have talked about a lot. In the absence of heavy-handed government and regulating, I think the absence of regulations is what has allowed the internet and the social media platforms to grow like they have. But I hate to sound cliché-ish, but that old line from the "Jurassic

Park” movie: Sometimes we are more focused on what we can do, and we don’t think about what we should do. And so I think that is where we find ourselves with some of this.

We have heard from some of our witnesses, accessibility of a global audience through internet platforms is being used for illegal and illicit purposes by terrorist organizations and even for the sale of opioids, which continues to severely impact communities across our Nation, particularly in rural areas like I live in, in eastern and southeastern Ohio.

However, internet platforms also provide an essential tool for legitimate communication and the free, safe, and open exchange of ideas, which has become a vital component of modern society and today’s global economy.

I appreciate hearing from all of our witnesses as our subcommittees examine whether Section 230 of the Communications Decency Act is empowering internet platforms to effectively self-regulate under this light-touch framework.

So, Mr. Huffman, in your testimony you discuss the ability of not only Reddit employees but its users to self-regulate and remove content that goes against Reddit’s stated rules and community standards. Do you think other social media platforms, for example, Facebook or YouTube, have been able to successfully implement similar self-regulating functions and guidelines? If not, what makes Reddit unique in their ability to self-regulate?

Mr. HUFFMAN. Sure. Thank you, Congressman.

I am only familiar with the other platforms to the extent that you probably are, which is to say I am not an expert. I do know they are not sitting on their hands. I know they are making progress.

But Reddit’s model is unique in the industry in that we believe that the only thing that scales with users is users. And so, when we are talking about user-generated content, sharing some of this burden with those people, in the same way that in our society here in the United States there are many unwritten rules about what is acceptable or not to say, the same thing exists on our platforms. And by allowing and empowering our users and communities to enforce those unwritten rules, it creates an overall more healthy ecosystem.

Mr. JOHNSON. OK.

Ms. Oyama, in your testimony you discuss the responsibility of determining which content is allowed on your platforms, including balancing respect for diverse viewpoints and giving a platform for marginalized voices. Would a system like Reddit’s up votes and down votes impact the visibility of diverse viewpoints on platforms like YouTube? And do dislikes on YouTube impact a video’s visibility?

Ms. OYAMA. Thank you for the question.

As you have seen, users can give thumbs up or thumbs down to a video. It is one of many, many signals, so it certainly wouldn’t be determinative in terms of a recommendation of a video on YouTube. That would mostly be for relevance.

And I really appreciate your point about responsible content moderation. I did want to make the point that, on the piece about harassment and bullying, we did remove 35,000 videos from

YouTube just in the last quarter, and we can do this because of CDA 230.

Whenever someone's content is removed, they may also be upset, so there could be cases against a service provider for defamation, for breach of contract. And service providers, large and small, are able to have these policies and implement procedures to identify bad content and take it down because of the provisions of CDA 230.

Mr. JOHNSON. OK. Well, I have got some other questions that I am going to submit for the record, Mr. Chairman, but let me just summarize with this, because I want to stay within my time, and you are going to require me to stay within my time.

So in the absence of regulations, as I mentioned in my opening remarks, that takes social responsibility to a much higher bar. And I would suggest to the entire industry of the internet, social media platforms, we better get serious about this self-regulating, or you are going to force Congress to do something that you might not want to have done.

With that, I yield back.

Mr. DOYLE. The gentleman yields back.

The Chair recognizes Ms. Matsui for 5 minutes.

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

I want to once again thank the witnesses for being here today.

Ms. Oyama and Mr. Huffman, last week the Senate Intel Committee released a bipartisan report on Russia's use of social media. The report found that Russia used social media platforms to sow social discord and influence the outcome of the 2016 election.

What role can Section 230 play in ensuring that platforms are not used again to disrupt our political process?

Ms. Oyama, Mr. Huffman, comments?

Ms. OYAMA. Thank you. Again, CDA 230 is critically important for allowing services like us to protect citizens and users against foreign interference in elections. It is a critical issue, especially with the election cycle coming up.

We found on Google across our systems in the 2016 election, fortunately, due to the measures we have been able to take and add removals, there were only two accounts that had infiltrated our systems. They had a spend of less than \$5,000 back in 2016.

We continue to be extremely vigilant. So we do publish a political ads transparency report. We require that ads are disclosed, who paid for them. They show up in a library. They need to be—

Ms. MATSUI. So you feel that you are effective?

Ms. OYAMA. We can always do more, but on this issue, we are extremely focused on it and working with campaigns to protect—

Ms. MATSUI. Mr. Huffman.

Mr. HUFFMAN. Yes, Congresswoman. So, in 2016, we found that the—we saw the same fake news and misinformation submitted to our platform as we saw on the others. The difference is, on Reddit it was largely rejected by the community, by the users, long before it even came to our attention.

If there is one thing Reddit is good at or our community is good at, it is being skeptical and rejecting also or questioning everything, for better or for worse.

Between then and now, we have become dramatically better at finding groups of accounts that are working in a coordinated or

inauthentic matter, and we collaborate with law enforcement. So based on everything we have learned in the past and can see going forward, I think we are in a pretty good position coming into the 2020 election.

Ms. MATSUI. OK.

Dr. Farid, in your written testimony, you mention the proliferation of mis- and disinformation campaigns designed to disrupt democratic elections. This sort of election interference really troubles me and a lot of other people.

You mentioned there is more that platforms could be doing about moderating content online. What more should they be doing about this issue now, this time?

Dr. FARID. Yes. So let me just give you one example. A few months ago, we saw a fake video of Speaker Pelosi make the rounds, OK, and the response was really interesting. So Facebook said, “We know it is fake, but we are leaving it up. We are not in the business of telling the truth.”

So that was not a technological problem, that was a policy problem. That was not satire. It was not comedy. It was meant to discredit the Speaker.

And so I think, fundamentally, we have to relook at the rules. And in fact, if you look at Facebook’s rules, it says you cannot post things that are misleading or fraudulent. That was a clear case where the technology worked, the policy is unambiguous, and they simply failed to implement the policy.

Ms. MATSUI. They failed. OK.

Dr. FARID. To YouTube’s credit, they actually took it down. And to Twitter’s discredit, they didn’t even respond to the issue.

So in some cases, there is a technological issue, but more often than not we are simply not enforcing the rules that are already in place.

Ms. MATSUI. So that is a decision they made—

Dr. FARID. Right.

Ms. MATSUI [continuing]. Nnot to enforce the rules.

OK.

Ms. Oyama and Mr. Huffman, what do you think about what Mr. Farid just said?

Mr. HUFFMAN. Sure. I will respond.

There are two aspects to this. First, specifically towards Reddit, we have a policy against impersonation.

Ms. MATSUI. OK.

Mr. HUFFMAN. So a video like that can both be used to manipulate people or serve as misinformation. It also raises question about the veracity of the things that we see and hear and prompts important discussions.

So the context around whether a video like that stays up or down on Reddit is really important, and those are difficult decisions.

I will observe that we are entering into a new era where we can manipulate videos. We have historically been able to manipulate text and images with Photoshop, and now videos.

So I do think not only do the platforms have a responsibility, but we as a society have to understand that the source of materials—for example, which publication—is critically important because

there will come a time, no matter what any of my tech peers say, where we will not be able to detect that sort of fakery.

Ms. MATSUI. Exactly.

And, Ms. Oyama, I know I only have 15 seconds.

Ms. OYAMA. Thank you.

I mean, on the specific piece of content that you mentioned, YouTube, we do have a policy against deceptive practices and removed it.

But there is ongoing work that needs to be done to be able to better identify deepfakes. I mean, of course, even comedians sometimes use them, but in political context or other places, it could severely undermine democracy. And we have opened up data sets, we are working with researchers to build technology that can better detect when media is manipulated in order for those policies to kick in.

Ms. MATSUI. Well, I appreciate the comment. I have a lot more to say, but you know how this is.

But anyway, I yield back the balance of my time. Thank you.

Mr. DOYLE. The gentlelady yields back.

The Chair recognizes Mr. Kinzinger for 5 minutes.

Mr. KINZINGER. Thank you, Mr. Chairman.

And thank you all for being here today. We very much appreciate it.

It is interesting, on the last line of questions, you know, one of the best things about democracy is our ability to have free speech and share opinions, but this can also be something that is a real threat. So I thank the chairman for yielding.

And I think it is safe to say that not every Member of Congress has a plan for what to do about Section 230 of the Communications Decency Act, but I think we all agree that the hearing is warranted. We need to have a discussion about the origins and intent of that section and whether the companies that enjoy these liability protections are operated in the manner intended.

And I will state up front that I generally appreciate the efforts certain platforms have made over the years to remove and block unlawful content. But I would also say that it is clearly not enough and that the status quo is unacceptable.

It has been frustrating for me in recent years that my image and variations of my name have been used by criminals to defraud people on social media, and this goes back 10 years, and literally, I think, could approach in the fifties to hundreds given on the ones that we just know about. These scams are increasingly pervasive, and I not only brought it up in the hearing with Mark Zuckerberg last year, I also wrote him again this summer to continue to press him to act more boldly to protect his users.

So I have a question. Sources indicate that in 2018 people reported hundreds of millions of dollars lost to online scammers, including \$143 million through romance scams. Given what so many people have gone through, it has become more and more important for platforms to verify user authenticity.

So both to Mr. Huffman and Ms. Oyama, what do your platforms do to verify the authenticity of user accounts?

Mr. HUFFMAN. Sure. Thank you for the question.

So there are again two parts to my answer. The first is on the scams themselves. My understanding is you are probably referring to scams that target veterans in particular.

We have a number of veterans communities on Reddit around support and shared experiences. They all, like all of our communities, create their own rules, and these communities have actually all created rules that prohibit fundraising generally, because the community and the members of those communities know that they can be targeted by this sort of scam in particular.

So that is the sort of nuance that we think is really important and highlights the power of our community model, because I, as a nonveteran, might not have had that same sort of intuition.

Now, in terms of what we know about our users, Reddit is not—we are different from our peers in that we don't require people to share their real world identity with us. We do know where they register from, what IPs they use, maybe their email address, but we don't force them to reveal their full name or their gender. And this is important, because on Reddit there are communities that discuss sensitive topics, in those very same veteran communities or, for example, drug addiction communities or communities for parents who are struggling being new parents. These are not things that somebody would go onto a platform like Facebook, for example, and say, "Hey, I don't like my kids."

Mr. KINZINGER. Yes, I understand. I don't mean to cut you off, but I want to go to Ms. Oyama.

Ms. OYAMA. Sure. And I am very sorry to hear that that happened to you, Congressman.

On YouTube we have a policy against impersonation. So if you were to ever see a channel that was impersonating you or a user saw that, there is a form where they can go in and submit. I think they upload their government ID, but that would result in the channel being struck.

On Search, spams can show up across the web. Search is an index of the web. We are trying to give relevant information to our users every single day on Search. We suppress 19 billion links that are spam, that could be scama, to defend the users. And then on Ads, we have something called the Risk Engine that can actually kick out bad or fraudulent accounts before they enter the system.

Mr. KINZINGER. Thank you.

And, you know, look, I am not upset about the sites that are, like, "Kinzinger is the worst Congressman ever," right, that is understandable, I guess, for some people. But when you have, again, in my case, somebody that flew—as an example, and there are multiple cases—flew from India using her entire life savings because she thought we were dating for a year, not to mention all the money that she gave to this perpetrator, and all these other stories.

I think one of the biggest and most important things is people need to be aware of that. If you have somebody over a period of a year dating you and never authenticated that, it is probably not real.

Ms. Peters, what are the risks associated with people not being able to trust other users' identities online?

Ms. PETERS. I think there are multiple risks of that, but I want to come back to the key issue for us, which is if it is illicit the sites

should be required to hand over data to law enforcement, to work proactively with law enforcement.

We have heard a lot today from the gentleman from Reddit about their efforts to better moderate. Some of our members were able to go online just the other day, type in a search for “buy fentanyl” online, and came up with many, many results. The same for “buy Adderall online,” “buy Adderall for cheap without prescription.”

Those are fairly simple search terms. I am not talking about a super high bar. To get rid of that on your platform doesn't seem too hard, or to have that automatically direct to a site that would advise you to get counseling for drug abuse.

We are not trying to be the thought police. We are trying to protect people from organized crime and terror activity.

Mr. KINZINGER. Thank you. And I will yield back, but I have a bunch more questions I will submit. Thank you.

Mr. DOYLE. The gentleman yields back.

And for the record, I want to say I don't think the gentleman is the worst Member of Congress. I don't even think you are at the very bottom, Adam. You are not a bad guy.

The Chair recognizes Ms. Castor for 5 minutes.

Ms. CASTOR. Well, thank you, Chairman Doyle, for organizing this hearing.

And thanks to all of our witnesses for being here today.

I would like to talk about the issue of 230 in the context of this horrendous tragedy in Wisconsin a few years ago and Armslist.com, where a man walked into a salon where his wife was working and shot her dead in front of their daughter and killed two others in that salon and then killed himself. And this is the type of horrific tragedy that is all too common in America today.

But, Dr. McSherry, you mentioned—I think you misspoke a little bit because you said that was all legal, but it wasn't, because 2 days before the shooting there was a temporary restraining order issued against that man. He went online shopping on Armslist.com 2 days after that TRO was issued, and the next day he commenced his murder spree.

And what happened is Armslist knows that they have domestic abusers shopping, they have got felons, they have got terrorists shopping for firearms, and yet they are allowed to proceed with this.

Earlier this year, the Wisconsin Supreme Court ruled that Armslist is immune even though they know that they are perpetuating illegal content in these kind of tragedies. They said, the Wisconsin Supreme Court ruled that Armslist is immune because of Section 230. They basically said it did not matter that Armslist actually knew or even intended that its website would facilitate illegal firearms sales to dangerous persons, Section 230 still granted immunity.

And then, Ms. Peters, you have highlighted that this is not an isolated incident. We are talking about child sexual abuse content, illegal drug sales. I mean, it has just—it has gone way too far.

So I appreciate that you all have proposed some solutions for this.

Dr. Citron, you have highlighted a safe harbor, that if companies use their best efforts to moderate content they would have some

protection. But how would this work in reality? Would this be, then, it is left up to the courts in those type of liability lawsuits, which kind of speaks to the need for very clear standards coming out of the Congress, I think?

Ms. CITRON. So yes, it would. And thank you so much for your question. How would we do this? It would be in the courts. So it would be an initial motion to dismiss. The company would then— whoever is being sued, the question would be: Are you being reasonable in your content moderation practices writ large, not with regard to any one piece of content or activity? And it is true that it would then, the enforcing mechanism, the 12(b)(6) motion in Federal court, have companies then explain what constitutes reasonableness.

Now, I think we can come up right now, with all of us, we have come up with some basic sort of threshold what we think is reasonable content moderation practices, what we might describe as technological due process. Transparency, accountability, clarity of what it is having a process, having clarity about what it is you prohibit.

But it is going to have to be case by case, context by context, because what is a reasonable response to a deepfake, and I have done a considerable amount of work on deepfakes, is going to be different from the kind of advice I would give to Facebook, Twitter, and others about what constitutes a threat and how one figures that out. How we can use—and I am thinking about Dr. Farid’s testimony about what we do about—there are certain issues—

Ms. CASTOR. And then let me—and it would be in the public interest, I believe, that if it is explicit illegal content, that they don’t—it wouldn’t wind up as an issue of fact in a lawsuit.

What do you think, Dr. Farid? If it is illegal content online, there really shouldn’t be a debatable question, right?

Dr. FARID. I am not a lawyer, to be clear, I am a mathematician by training, so I don’t think you really want to be asking me that question, but I completely agree with you. In some cases we have seen over the years, and we saw this when we were deploying PhotoDNA, is the technology companies want to get you muddled up in the gray area.

So we had conversations when we were trying to remove child abuse material saying: What happens when it is an 18-year-old? You know, what happens when it is not sexually explicit?

And my answer is, yes, those are complicated questions, but there is really clearcut bad behavior. We are doing awful things to kids as young as 2 months old. There is no issue.

Ms. CASTOR. I am going to interrupt you, because my time is short, and just going to highlight to the witnesses. There is also an issue with the number of moderators who are being hired to go through this content. A publication called The Verge had a horrendous story of Facebook moderators, and it caught my attention because one of the places is in Tampa, Florida, my district.

I am going to submit follow-up questions about moderators and some standards for that practice as follow-up, and I encourage you to answer and send it back. Thank you.

Mr. MCNERNEY [presiding]. The gentlelady yields.

Now the Chair recognizes the gentleman from Illinois, Mr. Shimkus, for 5 minutes.

Mr. SHIMKUS. Thank you, Mr. Chairman. It is great to be with you. I am sorry I missed a lot of this because I am upstairs. But in my 23 years being a Member, I have never had a chance to really address the same question to two different panels on the same day. So it was kind of an interesting convergence. Upstairs we are talking about e-vaping and underage use and what is in the product.

So I was curious, when we were in the opening statements here, someone, and I apologize, I am not sure, mentioned two cases. One was dismissed because they really did nothing, and one, the one who tried to be the good actor, got slammed. I don't know about slammed. But I see a couple heads being—Ms. Citron, can you address that first? You are shaking it the most.

Ms. CITRON. Yes, enthusiastically, because those are the two cases that effectively gave rise to Section 230. So what animates Chris Cox to go to Ron Wyden and say, you know, “We have got to do something about this” is two—a pair of decisions in which one basically says, if you do nothing you are not going to be punished for it, but if you try and you moderate, actually that heightens your responsibility.

Mr. SHIMKUS. So no good deed goes unpunished.

Ms. CITRON. Exactly. Right. So that is why we are in heated agreement about those two cases. That is why we are here today in many respects.

Mr. SHIMKUS. So, if I tie into this what is going on upstairs, and someone uses a platform to encourage underage vaping with unknown nicotine content, and the site then decides to clean it up, because of the way the law is written right now this good deed, which we most would agree that it probably is a good deed, would go punished?

Ms. CITRON. No, no. Now we have Section 230. That is why we have Section 230. They are encouraged, just so long as they are doing it in good faith, under section 230 (c)(2), they can remove it, and they are Good Samaritans.

Mr. SHIMKUS. Right. OK. So that is the benefit of it. Is there fear? OK. So in this debate that we heard earlier in opening comments from some of my colleagues in the USMCA debate, that part of that would remove the protections of 230, and then we would fall back to a regime by which the good-deed person could get punished. Is that correct? Everybody is kind of shaking their head mostly?

Ms. PETERS, you are not. Go ahead.

Ms. PETERS. We need to keep the 230 language out of the trade agreements. It is currently an issue of great debate here in the United States. It is not fair to put that in a trade agreement. It will make it impossible for—or make it harder for—

Mr. SHIMKUS. Well, don't get me wrong, I want USMCA passed as soon as possible without any encumbered work that doesn't happen, and I am not a proponent of trying to delay this process, but I am just trying to work through this debate. I mean, the concern upstairs to those of us—we believe in legal products that have been, me, approved by the FDA, and we are concerned about a black market operation that would then use platforms illicitly to

sell to underage kids. That would be how I would tie these two hearings together, which, again, I still think is pretty interesting.

When we had the Facebook hearing a couple years ago, I referred to a book called “The Future Computed,” which talks about the ability of industry to set those standards. I do think that industry—we do this across the board in a lot of this, whether it is engineering of heating and air cooling equipment or that. We do have industry that comes together for the good of the whole, for the good actors, and say, “Here are our standards.”

And the fear is that, if this sector doesn’t do that, then the heavy hand of government will do it, which I think would really cause a little more problem.

Dr. Farid, you are shaking your head.

Dr. FARID. We have been saying to the industry, “You have to do better because, if you don’t, somebody is going to do it for you. So you do it on your terms or somebody else’s terms.”

Mr. SHIMKUS. That would be us.

Dr. FARID. So do it on your terms. I agree.

Mr. SHIMKUS. We are not the experts.

So part of the book talks about fairness, reliability, privacy, inclusion, transparency, and accountability. I would encourage the industry and those who are listening to help us move in that direction on their own before we do it for them.

And with that, Mr. Chairman, I yield back my time.

Mr. MCNERNEY. The gentleman yields, and the Chair recognizes the chair for 5 minutes.

I would like to—I mean, it is very interesting testimony and jarring in some ways.

Ms. Peters, your testimony was particularly jarring. Have you seen any authentic offers of weapons of mass destruction being offered for sale online?

Ms. PETERS. I have not personally, but we certainly have members of our alliance that are tracking weapons activity. And I think what is more concerning to me in a way is the number of illegal groups, from Hezbollah, designated Hezbollah groups, to al-Qaida, that maintain web pages and links to their Twitter and Facebook pages from those and then run fundraising campaigns off of them. There are many, many—

Mr. MCNERNEY. I am just interested in the weapons of mass destruction issue.

Ms. PETERS. There are many platforms that allow for secret and private groups. It is inside—those groups are the epicenter of illicit activity. So it is hard for us to get inside those. We have actually run undercover operations to get inside some of them. But we haven’t gotten—

Mr. MCNERNEY. All right. Thank you, Ms. Peters.

Mr. Farid, in your testimony, you talked about the tension at tech companies between the motivation to maximize amount of time online on their platforms on the one hand, and on the other hand content moderation. Could you talk about that briefly, please?

Dr. FARID. So we have been talking a lot about 230, and that is an important conversation, but there is another tension point here, and there is another thing, which is the underlying business model of Silicon Valley today is not to sell a product. You are the product.

And in some ways that is where a lot of the tension is coming from, because the metrics we use at these companies for success is how many users and how long do they stay on the platforms. You can see why that is fundamentally in tension with removing users, removing content.

And so the business model is also at issue, and the way we deal with privacy of user data is also at issue here, because if the business model is monetizing your data, well, then I need to feed you information. There is a reason why we call it the rabbit hole effect on YouTube. There is a reason why, if you start watching certain types of videos of children or conspiracies or extremism, you are fed more and more and more of that content down the rabbit hole.

And so there is real tension there, and it is the bottom line. It is not just ideological. We are talking about the underlying profits.

Mr. MCNERNEY. OK.

Ms. Oyama, would you like to add to that?

Ms. OYAMA. Thank you.

I think many of these issues that we are discussing today, whether it is harassment, extremism, it is important to remember the positive and productive potential for the internet. On YouTube we have seen It Gets Better, we have seen countermessaging. We have a program called Creators for Change who are able to create really compelling content for youth to counter extremist messages.

And I think it is just good to remember the CDA 230 was born out of this committee. It has been longstanding policy. It is relevant to foreign policy as well. We would support its inclusion in USMCA or any other modern digital trade framework. It is responsible for the \$172 billion surplus the United States has in digital services. It is critically important for small businesses to be able to moderate content and to prevent censorship from other, more oppressive regimes abroad.

Mr. MCNERNEY. It is a great issue, and it is kind of hard to restrain yourself to brief answers. I understand that.

But clearly, companies could be doing more today within the current legal framework to address problematic content. I would like to ask each of you very briefly what you think could be done today with today's tools to moderate content, starting with Mr. Huffman. Very briefly, please.

Mr. HUFFMAN. Sure. So for us, the biggest challenge is evolving our policies to meet new challenges. But as such, we have evolved our policies a dozen times over the last couple years, and we continue to do so into the future. For example, two recent ones for us were expanding our harassment policy and banning deepfake pornography.

So undoubtedly there will be—"deepfake pornography" wasn't even a word 2 years ago. So undoubtedly there will be new challenges in the future, and being able to stay nimble and address them is really important. 230 actually gives us the space to adapt to these sorts of new challenges.

Mr. MCNERNEY. OK.

Ms. Citron.

Ms. CITRON. I would say so would a reasonableness standard. The nimbleness that reasonable enables is ensuring that we do respond to changing threats. The threats landscape is going to

change. We can't have a checklist right now. But I would encourage companies to not only have policies but be clear about them and to be accountable.

Mr. MCNERNEY. OK.

Dr. McSherry.

Dr. MCSHERRY. Just quickly, the issue for me with the reasonableness standard is, as a litigator, that is terrifying. That means as a practical matter, especially for a small business, a lot of litigation risk as courts try to figure out what counts as reasonable.

To your question, one of the crucial things I think we need if we want better moderation practices and we want users not to be treated just as products is to incentivize alternative business models. We need to make sure that we clear a space so there is competition so then, when a given site is behaving badly, such as Grindr, people have other places to go with other practices and they are encouraged to—you know, other sites are encouraged to develop and evolve. That will make—market forces sometimes can work. We need to let them work.

Mr. MCNERNEY. Thank you.

I am going to have to cut off my time now, and I am going to yield to the gentlelady from Indiana, Mrs. Brooks, for 5 minutes.

Mrs. BROOKS. Thank you, Mr. Chairman. Thank you so much for this very important hearing.

Dr. Farid, actually, to set the record, and the reason I am asking these questions, I am a former U.S. attorney. I was very involved in the Internet Crimes Against Children Task Force. We did a lot of work from 2001 to 2007.

And you are right, Mr. Huffman, deepfake pornography was not a term at that time.

And so we certainly know that law enforcement has been challenged for now decades in dealing with pornography over the internet. And yet, I believe that we have to continue to do more to protect children and protect kids all around the globe.

A concept, or tool, PhotoDNA, was developed a long time ago to detect criminal online child pornography, yet it means nothing to detect that illegal activity if the platforms don't do anything about it. And so now we have been dealing with this now for decades. This is not new. And yet, we now have new tools, right, so PhotoDNA. Is it a matter of tools or effort? Or how is it that it is still happening?

Dr. Farid.

Dr. FARID. I have got to say this is a source of incredible frustration. So first of all, I was part of the team that developed PhotoDNA back in 2008 with Microsoft. And I will tell you, for an industry that prides itself on rapid and aggressive development, there have been no tools in the last decade that have gone beyond PhotoDNA. That is pathetic, that is truly pathetic when we are talking about this kind of material.

How does an industry that prides itself on innovation say we are going to use 10-year-old technology to combat some of the most gut-wrenching, heartbreaking content online? It is completely inexcusable. This is not a technological limitation. This is we are simply not putting the effort into developing and deploying the tools.

Mrs. BROOKS. And let me just share that having watched some of these videos, it is something you never want to see and you cannot get out of your mind.

Dr. FARID. I agree.

Mrs. BROOKS. And so I am curious. Ms. Oyama, you wanted to respond, and how is it that we are still at this place?

Ms. OYAMA. Yes. Thank you for the question.

I mean, I will say at Google that is not true at all. We have never stopped working on prioritizing this. We can always do better. But we are constantly adopting new technologies. We initiated one of the first ones, which was called CSAI Match, which enabled us to create digital fingerprints of this imagery, prevent it from ever being reuploaded on YouTube, and we also share it with NCMEC.

And there is a new tool that we have called a Content Safety API, it is very new, and we are sharing it with others in the industry, with NGOs. It has resulted in a 7X increase in the speed at which this type of content is able to identify.

So it is going to continue to be a priority, but I just wanted to be clear that, from the very top of our company, we need to be a safe, secure place for parents and children, and we will not stop working on this issue.

Mrs. BROOKS. Well, and I am very pleased to hear that there have been advances then, and that you are sharing them, and that is critically important.

However, I will say that Indiana State Police Captain Chuck Cohen, who has actually testified before Energy and Commerce, recently told me that one of the issues that law enforcement runs into when working with internet companies is an attitude that he calls minimally compliant. And he said that internet companies will frequently not preserve content that can be used for investigation if law enforcement makes the companies aware of the concerning materials or automatically flags that content to law enforcement for review without actually checking if it is truly objectionable or not.

Do any of you have thoughts specifically on his comment? He has been an expert. Do any of you have thoughts on how we balance this law enforcement critical need? Because they are saving children all around the globe, Ms. Peters, without restricting companies' immunity from hosting concerning content.

Ms. PETERS. I just feel like if companies start getting fines or some sort of punitive damage every time there is illicit content, we are going to see a lot less illicit content very, very quickly. If it is illegal in real life, it should be illegal to host it online. And that is a very simple approach that I think we could apply industry-wide.

Mrs. BROOKS. And so I have a question, particularly because I asked Mark Zuckerberg this relative to terrorism and to recruitment and ISIS, and now we need to be even be more concerned about ISIS. And I understand that you have teams of people that take it down. How many people are on your team, Mr. Huffman?

Mr. HUFFMAN. Dedicated to?

Mrs. BROOKS. Removing content.

Mr. HUFFMAN. Removing contents at scale and writing our policies, it is about 20 percent of our company. It is about 100 people.

Mrs. BROOKS. Twenty percent of your company, about 100 people.

Ms. Oyama, how many people?

Ms. OYAMA. More than 10,000 people working on content moderation.

Mrs. BROOKS. That actually remove content?

Ms. OYAMA. That are involved in the content moderation, development of the policies, or the human—

Mrs. BROOKS. But how many people are on the team that actually do that work?

Ms. OYAMA. Again, I am happy to get back to you.

Mrs. BROOKS. OK. Thank you.

With that, I yield back. Thank you.

Mr. MCNERNEY. The gentlelady yields.

At this point I would like to introduce a letter for the record. Without objection, so ordered.

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

Mr. MCNERNEY. Next, the Chair recognizes the gentlewoman from New York, Ms. Clarke, for 5 minutes.

Ms. CLARKE. I thank our chairman and our chairwoman and our ranking members for convening this joint subcommittee hearing today on fostering a healthier internet to protect consumers.

I introduced the first House bill on deepfake technology, called the DEEPFAKES Accountability Act, which would regulate fake videos. Deepfakes can be used to impersonate political candidates, create fake revenge porn, and theater the very notion of what is real.

Ms. Oyama, Mr. Huffman, your platforms are exactly where deepfakes are shared. What are the implications of Section 230 on your deepfakes policies?

Mr. HUFFMAN. Sure, I will go. Thank you for the question.

So we released—actually, I think, with most of our peers around the same time—prohibition of deepfake pornography on Reddit because we saw that as a new, emerging threat that we wanted to get ahead of as quickly as possible.

The challenge we face, of course, is the challenge you raise, which is the increasing challenge of being able to detect what is real or not. This is where we believe that Reddit's model actually shines. By empowering our users and communities to adjudicate on every piece of content, they often highlight things that are suspicious, not just videos and images but also texts and news sources.

I do believe very strongly that we as a society, not just us as platforms, but in addition to, have to develop defenses against this sort of manipulation, because it is only going to increase.

Ms. CLARKE. Ms. Oyama.

Ms. OYAMA. Thank you.

Yes, on YouTube our overall policy is a policy against deceptive practices. So there has been instances where we have seen these deepfakes. I think the Speaker Pelosi video is one example where we identified that. It was a deepfake, and it was removed from the platform.

For both Search and for YouTube, surfacing authoritative, accurate information is core to our business, core to our long-term business incentives.

I would agree with what Mr. Huffman said, is that one of the things that we are doing is investing deeply in the academic side, the research side, the machine learning side to open up data sets where we know these are deepfakes and get better at being able to identify when content is manipulated.

We also do have a revenge porn policy for Search for users who are victimized by that, and we did also expand that to include synthetic images or deepfakes in that area, too.

Ms. CLARKE. Very well.

Ms. CITRON, could you discuss the implication of Section 230 on deepfakes monitoring and removal?

Ms. CITRON. Section 230, sort of the activities that we have seen YouTube and Reddit engage in, are precisely the kinds of activities that are proactive in the face of clear illegality, moving quickly.

But the real problem isn't these folks at the table. There are now—so Deeptrace Labs just issued a poll 2 weeks ago showing that 8 out of the 10 biggest porn sites have deepfake sex videos, and there are 4 sites now that basically their business model is deepfake sex videos and that 99 percent of those videos involve women.

Ms. CLARKE. So let me ask you. Does the—

Ms. CITRON. Section 230 provides them immunity because it is users posting them.

Ms. CLARKE. Does the current immunity structure reflect the unique nature of this threat?

Ms. CITRON. I don't think that—so, Section 230, as it is devised, it is, at its best, it is supposed to incentivize the kind of nimbleness that we are seeing for some dominant platforms. But it is not, the way the plain language is written under 230(c)(1), it doesn't condition the immunity on being responsible and reasonable. And so you have these outliers that cause enormous harm because it can be that in a search of your name that there is a deepfake sex video until it is, you know, de-indexed. And it is findable and people then contact you, and it is terrifying for victims.

So it is really these outlier companies that their business model is this kind of abuse, and Section 230 is what they point to when they gleefully say, "Sue me. Too bad, so sad." And that is the problem.

Ms. CLARKE. Very well.

One of the many issues that has become an existential threat to civil society is the rise of hate speech and propaganda on social media platforms.

Ms. Oyama, if 230 were removed, would platforms be liable for hosting distasteful speech, and would it change their incentives around moderating such speech?

Ms. OYAMA. Thank you for the question. I think this is a really important area to show the power and the importance of CDA 230.

I mean, as you know, there are First Amendment restrictions on government regulation of speech. So there is additional responsibility for service providers like us in the private sector to step up. We have a policy against hate speech. Incitement to violence is prohibited. Hate speech is prohibited, speech targeting hate at specific groups for attributes based on race, religion, veteran status, age.

And the takedowns that we do every single quarter through automated flagging, through machine learning, or through human reviewers are lawful and possible because of 230. When we take down content, someone's content is being taken down. And so they can regularly come back to any service provider, big or small. They may sue them for defamation or other things.

I think looking at the equities of the small business interests in this space would be really important as well, because I think they would say that they are even more deeply reliant on this flexibility and this space to innovate new ways to identify bad content and take it down without fear of unmitigated, you know, litigation, or legal risk, or legal uncertainty.

Ms. CLARKE. Very well. Thank you very much.

I yield back, Madam Chairman.

Ms. SCHAKOWSKY [presiding]. The gentlelady yields back.

And now, Mr. Walberg, you are recognized for 5 minutes.

Mr. WALBERG. I thank the chairwoman.

And I appreciate the panel being here.

Today's hearing and the issues at hand hit home for a lot of us, as we have discussed here. The internet is such an amazing, amazing tool. It has brought about great innovation, connecting millions of people in ways that were never even thought of before. And, I mean, truthfully we look forward to what we will see in the future. But these are issues we have to wrestle with.

Earlier this year I was pleased to invite Haley Petrowski from my district to the State of the Union as my guest to highlight her good work that she is doing in my district and surrounding areas to help combat cyberbullying, a very much comprehensive individual who understands so much as a young person of what is going on and is having a real impact in high schools and in colleges now as a result of her experience and trying to attempt to make some positive things out of it after she almost committed suicide, and thankfully it wasn't successful, as a result of cyberbullying. She has shined a light on that.

So, Mr. Huffman and Ms. Oyama, what are your companies doing to address cyberbullying on your platforms?

Mr. HUFFMAN. Sure. Thank you for the question, Congressman.

Just 2 weeks ago we updated our policies around harassments. It is one of the, I think, most complex or nuanced challenges we face because it appears in many ways.

One of the big changes we made is to allow harassment reports not just from the victim but from third parties. Basically, if somebody else sees instances of harassment, they will report it to us and our team so that we can investigate.

This is a nationwide issue, but particularly on our platform when people come to us in times of need. For example, a teenager struggling with their own sexuality has no place to turn, maybe not their friends, not their family, so they come to a platform like ours to talk to others in difficult situations; or people who are having suicidal thoughts come to our platform. And it is our first priority, regardless of the law, though we fully support lawmakers in this initiative, to make sure that those people have safe experiences on Reddit.

So we have made a number of changes, and we will continue to do so in the future.

Mr. WALBERG. OK.

Ms. Oyama.

Ms. OYAMA. Thank you for the question.

On YouTube, harassment and cyberbullying is prohibited. And so we would use our policies to help us enforce, and either through automated detection, human flagging, community flagging we would be able to identify that content and take it down. Last quarter we removed 35,000 videos under that policy against harassment and bullying.

And I did just want to echo Mr. Huffman's perspective that the internet and content sharing is also a really valuable place. It can serve as a lifeline to a victim of harassment or bullying. And we see that all the time when someone may be isolated in their school or somewhere else. Being able to reach out across borders to another State or to find another community has really created a lot of hope. And we also want to continue to invest in that important educational, mental health resources, content like that.

Mr. WALBERG. Well, I am glad to hear you both are willing to continue investing and helping us as we move forward in this area.

Ms. Oyama, Google's Ad network has come a long way in the last few years and won't serve ads next to potentially illegal activity. This is laudable and demonstrates Google has come a long way in identifying illegal activity. Given that Google is able to identify such activity, why would it not just take down the content in question?

Ms. OYAMA. [Inaudible.] I am sorry.

Mr. WALBERG. That was for Ms. Oyama, for you.

Ms. OYAMA. It is true that on our Ad system we do have a risk engine, and so we prohibit illegal content. There are many different policies, and they are stricken, more than 2 billion ads every year are stricken out of the Ad network for violating those policies, illegal and beyond.

Mr. WALBERG. So you are taking them down.

Ms. OYAMA. Yes, absolutely, before they are ever able to hit any page. I think it is very squarely in line with our business interests. We want advertisers to feel that our network, that our platforms are safe. Our advertisers only want to be serving good ads to good content.

Mr. WALBERG. One final question. I understand that Google offers a feature to put a tag on copyrighted work that would automatically take it down if pirated and uploaded, but that Google charges a fee for this. Can this technology be applied to other legal content? And why doesn't Google offer this tool for free?

Ms. OYAMA. Thank you for the question.

I think that may be a misperception, because we do have Content ID, which is our copyright management system. It is automated. We have partners across the music industry, film, I think every leading publisher is part of it. It is part of our partner program, so it is offered for free, and actually it doesn't cost the partners anything.

It is a revenue generator. So last year we sent \$3 billion based on Content ID claims of corrected material that right holders

claimed. They were able to take the majority of the ad revenue associated with that content and it was sent back out to them.

And that is system of being able to identify and detect algorithmically content, to then set controls, whether it should be in the entertainment space perhaps monetized and served or in the case of violent extremism absolutely blocked is something that powers much of YouTube.

Mr. WALBERG. Thank you. I yield back.

Ms. SCHAKOWSKY. The gentlemen yields back.

And, Mr. Loeb sack, you are recognized for 5 minutes.

Mr. LOEB SACK. Thank you, Madam Chair.

I do want to thank Chairman Doyle and Chair Schakowsky and the two ranking members of the subcommittees for holding this hearing today.

And I want to thank the witnesses for your attendance as well. This has been very informative, even if we are not able to answer all the questions we would like to be able to answer.

And it is not the first time our committee has examined how social media and the internet can be both a force for innovation and human connection—which we all enjoy when we are making those connections, so long as they are positive, obviously—but also a vector of harm and criminality.

I think everyone assembled here today is clearly very expert in your field, and I appreciate hearing from you all today as we consider how Section 230 has been interpreted by the courts since its initial passage and what, if any, changes we should be considering.

I think there is a lot to consider as we discuss the full scope of what Section 230 covers. From cyberbullying and hate speech, whether on Facebook, YouTube or elsewhere, to the illicit transaction of harmful substances or weapons, I think the question today is twofold.

First, we must ask if content moderators are doing enough. And, second, we must ask whether congressional action is required to fix these challenges. That second one has kind of been referred to obliquely throughout by some of you, by some of us, but I think that is essentially the second question that we are really facing today.

And after reviewing the testimony you have submitted, we clearly have some differences of opinion on whether Section 230 is where Congress should be focusing its resources.

So, to begin, I would like to ask everyone the same question, and this is probably at once the easiest question to answer and the most difficult because it is exceedingly vague. What does the difference between good and bad content moderation look like?

Start with you, Mr. Huffman.

Mr. HUFFMAN. Thank you, Congressman, for that philosophically impossible question, but I think there are a couple of easy answers that I hope everybody on this panel would agree with.

Bad content moderation is ignoring the problem. And that was the situation we were in pre-230, and that was the sort of perverse incentives we were facing.

I think there are many forms of good content moderation. What is important to us at Reddit is twofold. One, empowering our users and communities to set standards of discourse in their communities and amongst themselves. We think this is the only truly scalable

solution. And the second is what 230 provides us, which is the ability to look deeply in our platform to investigate, to use some finesse and nuance when we are addressing new challenges.

Mr. LOEBSACK. Thank you.

Ms. Citron.

Ms. CITRON. What was the question? To be about what makes bad—what makes content bad, or was it what makes—

Mr. LOEBSACK. Moderation.

Ms. CITRON. OK.

Mr. LOEBSACK. What is the difference between good and back content moderation.

Ms. CITRON. Moderation. OK.

Mr. LOEBSACK. Because that is what we are talking about.

Ms. CITRON. No, of course, but it precedes the question of why we are here. That is, what kinds of harms get us to the table to say why we should even try to talk about changing Section 230.

And I would say what is bad or incredibly troubling is when sites are permitted to have an entire business model which is abuse and harm. So, by my rights, that is the worst of the worst, and sites that induce and solicit illegality and harm, that to me is the most troubling.

Mr. LOEBSACK. And that is the problem. But then the question is how to deal with the problem in terms of moderation.

Ms. CITRON. And I have got some answers for you, but, you know, if we want to wait to do that.

Mr. LOEBSACK. You can submit them to us in writing if you would like.

Ms. CITRON. I did in my testimony.

Mr. LOEBSACK. I understand that.

Ms. CITRON. We have got to deal with the bad Samaritans and then a broader approach.

Mr. LOEBSACK. Thank you.

Ms. McSherry.

Dr. MCSHERRY. Thank you. Thank you for the question.

I actually think it is great question. And I think, as someone who supports civil liberties online as a primary goal for us, I think good content moderation is precise, transparent, and careful. What we see far too often is that, in the name of content moderation and making sure the internet is safe for everybody, actually all kinds of valuable and lawful content is taken offline.

There are details about this submitted in our testimony, but I would just point to one example where we have an archive of—there is an archive of videos attempting to document war atrocities, but those videos are often flagged as violating terms of service because, of course, they contain horrible material. But the point is to actually support political conversations, and it is very difficult for the service providers to apparently tell the difference.

Mr. LOEBSACK. Thank you.

Ms. Peters.

Ms. PETERS. If it is illegal in real life, it ought to be illegal online. Content moderation ought to focus on illegal activity. And I think there has been little investment in technology that would improve this for the platforms precisely because of Section 230 immunities.

Mr. LOEBACK. Thank you.

I do realize I am out of time. I am sorry I asked such a broad question of all of you, but I would like to get your response, if I could, the final two witnesses here, in writing, if I could, please.

Thank you so much. And I yield back. Thank you.

Ms. SCHAKOWSKY. The gentleman yields back.

And now I recognize Mr. Carter for 5 minutes.

Mr. CARTER. Thank you, Madam Chair.

And thank all of you for being here.

I know that you all understand how important this is, and I hope that you—and I believe you all take it seriously. So thank you for being here, and thank you for participating in this.

Ms. Peters, I am going start with you. I would like to ask you, in your testimony you pointed out that there is clearly quite a bit of illegal conduct that the online platforms still are hosting, for instance, illegal pharmacies where you can buy pills without a prescription, terrorists that are profiteering off of looted artifacts, and also products from endangered species. And then it even gets worse. You mentioned the sale of human remains and child exploitation, I mean, just gross things, if you will.

How much effort do you feel like the platforms are putting into containing this and to stopping this?

Ms. PETERS. Well, it depends on the platform. But that is a very good question. And I would like to respond with a question to you and to the committee: When was the last time anybody here saw a dick pic on Facebook? Simple question.

If they can keep genitalia off of these platforms, they can keep drugs off these platforms. They can keep child sexual abuse off these platforms. The technology exists. These are policy issues, whether it is the policy to allow the video of Nancy Pelosi on or the policy to allow pictures of human genitalia.

Mr. CARTER. I get it. I understand.

Let me ask you this. Do you ever go to them and meet with them and express this to them?

Ms. PETERS. Absolutely.

Mr. CARTER. And how are you received?

Ms. PETERS. We are typically told that the firm has quite intelligent people working on it, that they are creating AI, and that in a few years that AI is going to work. And when we have presented evidence of specific, identifiable crime networks and terror networks, we have been told that they will get back to us, and then they don't. That has happened multiple times.

Mr. CARTER. Are you ever told that they don't want to meet with you? I mean—

Ms. PETERS. No, we have usually gotten meetings or calls.

Mr. CARTER. So you feel like you got a good relationship. Do you feel like the effort is being put forth?

Ms. PETERS. I don't feel like effort is being put forth. I feel like—

Mr. CARTER. You see, that is where I struggle, because I don't want the—you know, I am doing my best to keep the Federal Government out of this. I don't want to stifle innovation, and I am really concerned about that.

But at the same time, look, we cannot allow this to go on. This is irresponsible. And if you don't do it, then you are going to force us to do it for you, and I don't want that to happen. I mean, it is just as clear as that.

Let me ask, Ms. Peters, you also mentioned in your testimony that you were getting funding from the State Department to map wildlife supply chains, and that is when you discovered that there was a large retail market for endangered species that exists on some platforms like Facebook and WeChat. Have any of these platforms made a commitment to stop this? And if they have, is it working? It getting any better?

Ms. PETERS. I mean, that is a terrific example to bring up, sir. A number of tech firms have joined a coalition with World Wildlife Fund and IFAW and have taken a pledge to remove endangered species content and wildlife markets from their platforms by 2020.

I am not aware that anything has changed. We have researchers going online and logging wildlife markets all the time.

Mr. CARTER. All right. I am going to be fair. OK. I am going to be fair and I am going to let the Google—I am sorry, I can't see that far—I am going to let you respond to that.

Do you feel like you are doing everything you can?

Ms. OYAMA. Thank you.

We can always do more. I think we are committed to always doing more.

Mr. CARTER. I appreciate that. I know that. I don't need you to tell me that. I need you to tell me "We have got a plan in place, and it is fixed" and then stop this.

Ms. OYAMA. Let me tell what you we are doing in the two categories that you mentioned.

So for wildlife, the sale of the endangered species is prohibited from Google Ads, we are part of the coalition that Ms. Peters mentioned.

On the national epidemic that you mentioned for opioids, we are hugely committed to helping and playing our part in combating this epidemic.

So there is an online component and an offline component. The online component, the research has showed that less than 0.05 percent of misuse of opioids originates on the internet. And what we have done, especially with Google Search, is work with the FDA. So the FDA can send us a warning letter if they see that there is a link in Search for a rogue pharmacy, and we will delist that out of Search.

There is a really important offline component, too. So we work with the DEA on Prescription Takeback Day. We feature these places in Google Maps, on CBS. Happy to come in and—

Mr. CARTER. OK. And I invite you to do just that, OK. I would like to see you and talk to you further about this.

Mr. Huffman, I am going to give you the opportunity, because we have gone, my staff has gone on Reddit, and they have Googled, if you will, or searched for illegal drugs, and it comes up. And I suspect you are going to tell me the same thing: We are working on it. We have almost it got it under control. But it is still coming up.

Mr. HUFFMAN. I have got a slightly different answer, if you will indulge me.

First of all, it is against our rules to have controlled goods on our platform, and it is also illegal. 230 doesn't give us protection against criminal liability.

We do see content like that on our platform. And, in fact, if you went to any technology service with a search bar, including your own emails, and typed in "buy Adderall," I am sure you would find a hit in your spam folder at least, and that is the case on Reddit as well.

That sort of content that has come up today is spam first gets removed by our filters, but there is a lag sometimes between something being submitted and something being removed. Naturally, that is how the system works.

That said, we do take this issue very seriously, and so our technologies have continued to improve along these lines. And that is exactly the sort of ability that 230 gives us, is the ability to look for this content and remove it.

Now, to the extent that you or your staff have found this content specifically, and to the extent that it is still on our platform, we would be happy to follow up later, because it shouldn't be.

Mr. CARTER. You know, my sons are grown now, but I feel like a parent pleading with their child again: Please don't make me have to do this.

Thank you, Madam Chair. I yield back.

Ms. SCHAKOWSKY. The gentleman yields back.

And now I recognize Congresswoman Kelly for 5 minutes.

Ms. KELLY. Thank you, Madam Chair. Thank you for holding this important hearing on Section 230 and fostering a healthier, more consumer-friendly internet.

The intended purpose of Section 230 was to allow companies to moderate content under the Good Samaritan provision, and yet this law seems to be widely misapplied. The Good Samaritan provision in Section 230 was intended "in good faith to restrict access or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."

Last Congress, Section 230 was amended through SESTA and FOSTA to make platforms liable for any activity related to sex trafficking. Since passage, some have criticized the law for being too ambiguous.

In addition to my work on this committee, I chair the House Tech Accountability Caucus. In that capacity, I have sought to work with stakeholders to protect family users in an accountable manner while allowing innovators to innovate.

Today, as we look to foster a healthier, more consumer-friendly internet, it is my hope our discussion will set the standard of doing so in a responsible, effective, and balanced way.

Professor Citron, in your testimony you discussed giving platforms immunity from liability if they could show that their content moderation practices writ large are reasonable. As the chairman referenced, how should companies know where the line is or if they are doing enough? Where is that line?

Ms. CITRON. And the sort of genius of reasonableness is that it matters and depends on the context. There are certainly some

baseline presumptions, I would say defaults, about what would constitute reasonable content moderation practices, and that includes having them. There are some sites that don't engage in that at all. In fact, they absolutely don't engage in moderation, and they encourage abuse and illegality.

But there are some baseline, I think, academic writing for the last 10 years and work I have done with companies for 10 years is there is a baseline set of speech rules and policies that we have seen that are best practices, but naturally that is going to change, depending on the challenge.

So we are going to have different approaches to different new and evolving challenges. And that is why a reasonableness approach which preserves the liability shield, right, but it does it in exchange for those efforts.

Ms. KELLY. And would you agree that any changes we make, we have to ensure that it doesn't further ambiguity?

Ms. CITRON. Right. And I think just to, if I may, about FOSTA and SESTA, what was disappointing to someone who certainly helped some offices work on the language is when you included the language "knowingly facilitate," that is the moderator's dilemma, that is, to either sit on your hands or to be overly aggressive.

And so my biggest disappointment was unfortunately how it came out, because we do see—we almost see ourselves back to Prodigy and CompuServe, those initial cases, and either we are seeing way overly aggressive responses to sexual expression online, which is a shame, and we see the doing nothing. So I hope we don't do that.

Ms. KELLY. Thank you.

The way people communicate is changing rapidly, as we all know. Information can start on one platform and jump to another and go viral very quickly. The 2016 election showcased how false information can spread and how effective it can be to motivate or deter different populations. Often offensive content is first shared in groups and then filtered out to a wider audience.

Ms. Peters, what do you believe is the responsibility of tech companies to monitor and proactively remove content that is rapidly spreading before being flagged by users?

Ms. PETERS. I believe that companies need to moderate and remove content when it concerns a clearly illegal activity. If it is illegal in real life, it ought to be illegal to host it online. Drug trafficking, human trafficking, wildlife trafficking, serious organized crime, and designated terror groups should not be given space to operate on our platforms.

I also think that CDA 230 needs to be revised to provide more opportunities for State and local law enforcement to have the legal tools to respond to illicit activity. That is one of the reasons FOSTA/SESTA was passed.

Ms. KELLY. And Ms. Oyama and Mr. Huffman, what steps are you taking beyond machine learning to stop the spread of extremist or misinformation content that is being shared widely? Are there flags that pop up if the same content is shared 10,000 or 100,000 times?

Ms. OYAMA. Yes. Thank you for the question.

So on YouTube we are using machines and algorithms. Once content is identified and removed, our technology prevents it from being reuploaded.

But I think to your really important point about working across platforms and cross-industry collaboration, a good example would be the GIFCT, the Global Internet Forum to Counter Terrorism. We are one of the founding members. Many of the leading players in tech are part of that.

One of the things that we saw during the Christchurch shooting was how quickly this type of content can spread. And we were grateful to see that last week some of the crisis protocols we put into place kicked in. So there was a shooting in Germany. There was a piece of content that appeared on Twitch, and the companies were able to engage in the crisis protocol. There was a hash made of the content, it was spread across the companies, and that enabled all of us to block it.

Ms. KELLY. And now I am out of time.

Thank you.

Ms. SCHAKOWSKY. The gentlelady yields back.

And Mr. Bilirakis is recognized for 5 minutes.

Mr. BILIRAKIS. Thank you, Madam Chair. I appreciate it very much.

My first question is for Dr. McSherry, a yes or no. I understand in the past EFF has argued for including language mirroring legislation in trade deals explicitly for the purpose of baking language into an agreement to protect the statute domestically. Do you see the intent of including such 230-like language in trade agreements is to ensure that we may not revisit the statute?

Dr. MCSHERRY. No.

Mr. BILIRAKIS. OK. All right. Thank you very much.

And then what I would like to do, Madam Chair, I would like to ask that EFF, the blog post from January 23, 2018, by Jeremy Malcolm, be entered into the record.

Ms. SCHAKOWSKY. Without objection, so ordered.

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

Mr. BILIRAKIS. Thank you, Madam Chair. I appreciate it.

The next question is for Mr. Huffman and Ms. Oyama. In April 2018, I questioned Mark Zuckerberg about how soon illegal opioid ads would be removed from their website. His answer was that the ads would be reviewed when they were flagged by users as being illegal or inappropriate. This, of course, is a standard answer in the social media space.

However, Mr. Zuckerberg also said at the time that industry needs to, and I quote, “build tools that proactively go out and identify ads for opioids before people even have to flag them for us to review,” and that ends the quote. This would significantly, in my opinion, cut down the time an illegal ad would be on their website.

Again, Mr. Huffman and Ms. Oyama, it has been a year and a half. This is an epidemic, and people are dying. I am sure you will agree with this. Has the industry been actively working on artificial intelligence flagging standards that can automatically identify illegal ads? And then what is the status of this technology, and when can we expect implementation, if they have been working on it?

Whoever would like to go first is fine.

Mr. Huffman.

Mr. HUFFMAN. Sure. Thank you, Congressman.

So Reddit is a little different than our peers in that all of our ads go through a strict human review process, making sure that not only are they on the right side of our content policy, which prohibits the buying and selling of controlled substances, but also our much more strict ads policy, which has a much higher bar to cross because we do not want ads that cause any sort of controversy on our platform.

Mr. BILIRAKIS. OK. But, I mean, you know, we have to be proactive as far as this is concerned, and Mr. Zuckerberg indicated that that is the case. You know, these kids are dying, people are dying, and we just can't stand by and have this happen and have access to these, well, in most cases opioids and drugs, different types of drugs.

But, Ms. Oyama, would you like to comment, please?

Ms. OYAMA. Thank you.

We certainly agree with your comment about the need for proactive efforts. So on Google Ads we have something called a risk engine that helps us identify if an ad is bad when it is coming into the system. We can kick it out. Last year, in 2018, we kicked out 3.2 billion ads out of our system for violating our policies.

For any prescription that would show up in an ad, that is also independently verified by an independent group called LegitScript. So that would need to also be verified by them.

And then, of course, in the specific case of opioids, those are a controlled substance under Federal law. So, there is a lot of important work that we have done with the DEA, with the FDA, even with pharmacies like CVS offline to help them promote things like Take Back Your Drugs Day where people can take opioids in and drop them off so they are not misused later on.

One of the things that we have seen is that the vast majority, more than 99 percent of opioid misuse, happens in the offline world, so from a doctor that is prescribing it or a family member or a friend. And so using technology to also educate and inform people that might be potentially victimized from this is equally important to some of the work that we are doing in the ad space.

Mr. BILIRAKIS. OK. How about anyone else on the panel, would they like to comment? Is the industry doing enough?

Ms. PETERS. I don't think the industry is doing enough. There is an enormous amount of drug sales taking place on Google Groups, on Instagram, on Facebook groups. The groups on these platforms are the epicenter, and this is why industry has to be monitoring this. If you leave this up to users to flag it and they are inside a private or a secret group, it is just not going to happen.

These firms know what users are getting up to. They are monitoring all of us all the time so they can sell us stuff. They can figure this out.

Dr. FARID. Congressman, can I also add there are two issues here. There are the ads, but there is also the native content. So you heard Ms. Peters say that she went this morning and searched on Reddit, and that content is there, even if it is not in the ads, and the same is true on Google Search. I can search for this. So there

are two places you have to worry about these things, not just the ads.

Mr. BILIRAKIS. Very good.

All right. Thank you, Madam Chair. I yield back.

Ms. SCHAKOWSKY. The gentleman yields back.

And now I call on the chairman of our full committee for 5 minutes, Mr. Pallone.

Mr. PALLONE. Thank you, Madam Chair.

I wanted to start with Ms. Oyama. In your written testimony you discuss YouTube's community guidelines for hate speech, and I am concerned about news reports that hate speech and abuse is on the rise on social media platforms.

How does Section 230 incentivize platforms to moderate such speech? And does Section 230 also incentivize platforms to take a hands-off approach to removing hate speech, if you will?

Ms. OYAMA. Thank you so much for the question.

So on the category of hate speech, YouTube prohibits hate speech. We have a very clear policy against it. So that would be speech that incites violence or speech that is hateful against groups with specific attributes. So that could be speech based on their race, their religion, their sex, their age, their disability status, their veteran status.

And so that is prohibited. It can be either detected by our machines, which is the case in more than 87 percent, by community flaggers, by individual users. And all of those actions that we take, last quarter, we saw a 5X increase in the amount of content that our machines were able to find and remove. Those removals are vitally dependent on the protection in CDA 230 to give service providers the ability to moderate content, to flag bad content, and to take it down.

We do have claims against us when we remove speech. People may sue us for defamation. They may have other legal claims. And 230 is what enables not only Google or not only YouTube but any site with user comments, with user-generated content, any site on the internet, large or small, to be able to moderate that content.

So I think we would just encourage Congress to think about not harming the good actors, the innocent actors that are taking these steps in an effort to go after a truly bad criminal actor where criminal law is fully exempted from the scope of the CDA 230. And they should be penalized, and law enforcement will play a really important role in bringing them down, as they did with Backpage that was taken down or on civil cases like Roommates.com where there is platform liability for bad actors that break the law.

Mr. PALLONE. Thank you.

Dr. Farid, in your written testimony you state that the internet has led to the proliferation of domestic and international terrorism. As you may know, there is both criminal and civil liability associated with providing material support for terrorism.

But I want to start with Dr. McSherry. Understanding that Section 230 doesn't apply to Federal criminal law, have U.S. social media companies used 230 to shield themselves from civil liability for allowing their platforms to be used as propaganda in recruitment platforms for terrorists with regard to civil liability?

Dr. MCSHERRY. So there are ongoing cases, and there have been several cases where platforms have been accused of violating civil laws for hosting certain kinds of content on their platforms, and they have invoked Section 230 in those cases quite successfully.

And I think that is not—if you look at the facts of a lot of those cases, that is actually quite appropriate. The reality is, it's very difficult for a platform to always be able to tell in advance, always draw the line in advance between content that is talking, that is simply protected political communications, and content that steps over a line. So these cases are hard, and they are complicated, and they have to get resolved on their facts.

Section 230, though, also creates a space in which, because of the additional protections that it provides, it creates a space for service providers when they choose to, to moderate and enforce their own policies.

Mr. PALLONE. Let me go back to Dr. Farid.

Do you have any thoughts on how this should be addressed from a technological perspective?

Dr. FARID. I want to start by saying, when you hear about the moderation that is happening today—we have heard it from Google, we have heard it from Reddit—you should understand that has only come after intense pressure. It has come from pressure from advertisers. It has come from pressure on Capitol Hill. It has come from pressure in the EU. And it has come from pressure from the press. So there is bad news, there is bad PR, and then we start getting serious.

For years we have been struggling with the social media companies to do more about extremism and terrorism online, and we have hit a hard wall. And then the EU started putting pressure. Capitol Hill started putting pressure. Advertisers started putting pressure. And we started getting responses.

I think this is exactly what this conversation is about, is what is the underlying motivating factor? The self-regulation of “trust us, we will do everything” is not working. So the pressure has to come from other avenues.

And I think putting pressure by modest changes to CDA 230 is the right direction. And I agree with Ms. Oyama, is that if these are good actors, then they should encourage that change and help us clean up and deal with the problems that we are dealing with.

I have been in this fight for over a decade now, and it is a very consistent pattern. You deny the problem exists, you minimize the extent of it, you deny the technology exists, and eventually you get enough pressure and then we start making changes. I think we should skip to the end part of that and just recognize that we can do better, and let's just start doing better.

Mr. PALLONE. Thank you.

Thank you, Madam Chair.

Ms. SCHAKOWSKY. The gentleman yields back.

And now I recognize for 5 minutes Congressman Gianforte.

Mr. GIANFORTE. Thank you, Madam Chair.

And thank you for being here today.

About 20 years ago I harnessed the power of the internet to launch a business to improve customer service. That company was called RightNow Technologies. And from a spare bedroom in our

home, we eventually grew that business to be one of the largest employers in Montana. We had about 500 high-wage jobs there.

The platform we created had about 8 million unique visitors per day. And I understand how important Section 230 can be for small business. This important liability shield has gotten mixed up, however, with complaints about viewpoint discrimination.

And I want to cite one particular case. In March of this year, Missoula-based Rocky Mountain Elk Foundation reached out to my office because Google had denied one of their advertisements. The foundation did what it had done many times. They had tried to use paid advertising on the Google network to promote a short video about a father hunting with his daughter.

This time, however, the foundation received an email from Google, and I quote: "Any promotions about hunting practices, even when they are intended as a healthy method of population control or conservation, is considered animal cruelty and deemed inappropriate to be shown on our network."

The day I heard about this, I sent a letter to Google and you were very responsive, but the initial position taken was absurd. Hunting is a way of life in Montana, in many parts of the country. I am very thankful that you worked quickly to reverse that, but I remain very concerned about Google's effort to stifle the promotion of Rocky Mountain Elk Foundation, and how they were treated. I worry that other similar groups have faced similar efforts to shut down their advocacy.

We really don't know how many hunting ads Google has blocked in the last 5 years. In my March letter, I invited Google's CEO to meet with leaders of our outdoor recreation businesses in Montana. I haven't heard anything back.

And, Ms. Oyama, I would extend the invitation again.

I think, frankly, it would help Google to get out of Silicon Valley, come to Montana, sit down with some of your customers, and hear from them directly about the things that are important to them. I would be happy to host that visit. We would love to meet with you there.

I think it is important to understand the work that these groups do to further conservation and to help species thrive. And as an avid hunter and outdoorsman myself, I know many businesses in Montana focus on hunting and fishing. And I worry they may be denied the opportunity to advertise on one of the largest online platforms that you have built, to your credit.

I also worry that an overburdensome regulatory regime could hurt small businesses and stifle Montana's rapidly growing high-tech sector. So the invitation is open.

Dr. Farid, one question for you. How can we walk this line between protecting small business and innovation versus overburdensome regulations?

Dr. FARID. It is absolutely the right question to ask, Congressman. I think you have to be very careful here, because right now we have near monopolies in the technology sector. And if we start regulating now, the small companies coming up are not going to be able to compete.

There are ways of creating carveouts. In the EU and the U.K., as they are talking about regulations, they are creating carveouts for small platforms that have 8 million versus 3 billion users.

So I do think we want to tread very lightly here. I think Ms. Peters also made the point that we want to inspire competition for better business models and allow these small companies. But I think there are mechanisms to do that. We just have to think carefully about it.

Mr. GIANFORTE. We have had a lot of discussion today about the efforts you are taking to get criminal activity off the network, so I applaud that. We should continue to do that.

But as a follow-on, Doctor, how do we ensure that content moderation doesn't become censorship and a violation of our First Amendment?

Dr. FARID. Good. So the way we have been thinking about content moderation is a collaboration between humans and computers. What computers are very good at doing is the same thing over and over and over again, but what they are not good at still is nuance and subtlety and complexity and inference and context.

So the way content moderation works today, for example, in the child sexual abuse space is human moderators say "this is a child, this is sexually explicit." We fingerprint that content, and then we remove very specifically and very targeted that piece of content.

False alarm raids for PhotoDNA that we developed a decade ago are about 1 in 50 billion. That is the scale you need to be operating at. So if you are going to deploy automatic technology, you have to be operating at very high scale. And so the humans—the computers can't do that on their own, so we need more human moderators.

You heard from Google, 10,000 moderators. There are 500 hours of video uploaded a minute. That is not enough moderators. You can do the arithmetic yourself. Those moderators would have to be looking at hours and hours of video per hour. So we have to also beef up our human moderation.

Mr. GIANFORTE. OK. Thank you.

And, Ms. Oyama, I look forward to seeing you in Montana.

And I yield back.

Ms. SCHAKOWSKY. The gentleman yields back.

And now I recognize—Congresswoman Blunt Rochester is next for 5 minutes.

Ms. BLUNT ROCHESTER. Thank you, Madam Chairwoman.

And to the chairmen and ranking members, thank you for holding this important hearing.

I think many of us here today are seeking to more fully understand how Section 230 of the Communications Decency Act can work well in an ever-changing virtual and technological world. This hearing is really significant, and as Ms. Oyama said, I want us to not forget the important things that the internet has provided to us, from movements to applications to TikTok.

But also, as Mr. Huffman said, we—and you applied it to Reddit, but I think it applies to all of us—must constantly be evolving, our policies must be evolving to face the new challenges while also balancing our civil liberties. So we have a really important balance here.

So my questions really are surrounded around this, the question that Mr. Loeb sack asked about bad content moderation. And I want to start off by saying that the utilization of machine-learning algorithms and artificial intelligence to filter through content posted on websites as large as YouTube provides an important technological solution to increasing the amount of content to moderate.

However, as we become more and more reliant on algorithms, we are increasingly finding blind spots and gaps that may be difficult to breach with simply more and better code.

I think there is a real concern that groups already facing prejudice and discrimination will be further marginalized and censored. And as I thought about this, I even thought about groups like the veterans or the African-American community in the 2016 elections.

Dr. Farid, can you describe some of the challenges with moderation by algorithm, including possible bias?

Dr. FARID. Yes. So I think you are absolutely right, Congresswoman. When we automate at the scale of the internet, we are going to have problems, and we have already seen that. We know, for example, that face recognition does much, much worse on women, on people of color than it does on White men.

The problem with the automatic moderation is that it doesn't work at scale. When you are talking about billions of uploads, and if your algorithm is 99 percent accurate—which is very, very good—you are still making 1 in 100 mistakes. That is literally tens of millions of mistakes a day you are going to be making at the scale of the internet.

And so the underlying idea that we can fully automate this, not to take on the responsibility and the expense of hiring human moderators simply doesn't work. And so I fear that we have moved too far to the "Give us time to find the AI algorithms because we don't want to hire the human moderators because of the expense."

And we know today that is not going to work in the next year, 2 years, 5 years, 10 years. And it is a little bit worse than that, because it also assumes an adversary that is not adapting, and we know that the adversaries can adapt. So we know, for example, that all machine learning and AI algorithms today that are meant to identify content are vulnerable to what are called adversarial attacks. You could add small amounts of content to the information, and you can completely fool the system.

Ms. BLUNT ROCHESTER. I want to ask a quick question of Mr. Huffman and Ms. Oyama. Both of you talked about the number of human moderators that you have available to you, and I know that we have had many hearings on challenges of diversity in the tech field.

I am assuming, Mr. Huffman, yours are more from the user perspective in terms of moderators, or are they people that you hire, and the 10,000 or so that you mentioned, these are people that you hire or are they users? Just a quick—so everybody knows—users, combination?

Mr. HUFFMAN. For us, it is about 100 employees out of 500, and, of course, millions of users participate as well.

Ms. BLUNT ROCHESTER. Got you. That is what I thought.

OK. Same?

Ms. OYAMA. So the 10,000 set that I mentioned is the mixture of the full-time employees. We also work with specialized vendors. And then we also have community flagging, which could be an NGO, could be law enforcement, could be an average user.

Ms. BLUNT ROCHESTER. OK. I know in the interest of time, I don't have a lot of time, but could you provide us with information on the diversity of your moderators? That is one of my questions.

And then also, I don't like to make assumptions, but I am going to assume that it might be a challenge to find diverse populations of individuals to do this role, what you are doing in that vein. So if we could have a follow-up with that.

And then my last question is just going to be for the panel. What should the Federal Government, what should we be doing to help in this space? Because I am really concerned about the capacity to do this and do it well. If anybody has any suggestion, recommendation. Mr. Farid is already pushing his button.

Dr. FARID. I think this conversation is helping. I think you are going to scare the bejesus out of the technology sector, and I think that is a really good thing to do.

Ms. BLUNT ROCHESTER. OK. I have to yield back. I am out of time. But thank you so much to all of you for your work.

Ms. SCHAKOWSKY. The gentlewoman yields back.

And now, last but not least, Representative Soto, you are recognized for 5 minutes.

Mr. SOTO. Thank you, Madam Chairwoman.

First of all, thank you for being here. I am the last one, so you are in the homestretch here.

It is amazing that we are here today when we think about how far the internet has progressed. One of the greatest inventions in human existence, connecting the world, giving billions a voice, while before their stories would never be told, providing knowledge at our fingerprints. It is just incredible.

And we know Section 230 has been a big part of it, providing that safe harbor against a dam, essentially the dam holding back the flood of lawsuits. It has created innovation. But it has also created a breeding ground for defamation and harassment, for impersonation and election interference, and also a breeding ground for White supremacists, disinformation, global terrorism, and other extremism.

So we have these wonderful gifts to humanity on one side and then all the terrible things with humanity on the other side.

My biggest concern is that lies spread faster than the speed of light in the internet, while truth seems to go at a snail's pace on it. So that is one thing that I constantly hear from my constituents.

So I want to start with some basics just so I know everybody's opinion on it. Who do you all each think should be the cop on the beat to be the primary enforcer, with the choices being FCC, FTC, or the courts? And it would be great to go down the line to hear what each of you think on that.

Mr. HUFFMAN. If those are my only three options, I would choose—

Mr. SOTO. You could give a fourth if you could give a few-word answer.

Mr. HUFFMAN. I think, in the United States, society, and on our platform, our users.

Mr. SOTO. OK. Who do you think should be the cop on the beat?

Ms. CITRON. I am going to take your second-best option, which is the courts.

Mr. SOTO. The courts.

Ms. CITRON. Because it forces in some sense the companies actually to be the norm producers.

Mr. SOTO. OK. Dr. McSherry.

Dr. MCSHERRY. Yes. So I think the courts have a very important role to play, but also a cardinal principle for us at EFF is, at the end of the day, users should be able to control their internet experience.

Mr. SOTO. OK.

Dr. MCSHERRY. We need to have many, many more tools to make that possible.

Mr. SOTO. Ms. Peters.

Ms. PETERS. I think that is a ridiculous argument. The vast majority of people—I study organized crime.

Mr. SOTO. Well, let's get back to—

Ms. PETERS. Hold on. I am going to answer the question: Courts and law enforcement.

Mr. SOTO. Thank you.

Ms. PETERS. Most people are good. A small percentage of people statistically in any community commit crime.

Mr. SOTO. OK. Ms. Oyama.

Ms. PETERS. You have to control for it.

Mr. SOTO. Thank you.

Ms. Oyama.

Ms. OYAMA. Content moderation has always been a multistakeholder approach, but I wanted to point out that the courts and the FTC do have jurisdiction. And, as you know, the FTC does have broad jurisdiction over tech companies already, and the courts are always looking at the outer contours of CDA 230.

Mr. SOTO. Thank you.

Dr. Farid.

Dr. FARID. I agree it is a multistakeholder. We all have a responsibility here.

Mr. SOTO. And if we were to tighten up rules on the courts, it would be great to hear, first starting with you, Dr. Farid, if—limit it to injunctive relief—do you think that would be enough, and whether or not there should be attorney's fees at stake.

Dr. FARID. Please understand, I am not a policymaker, I am not a lawyer. I am a technologist. I am not the one who should be answering that question, with due respect.

Mr. SOTO. OK. Ms. Oyama and Mr. Huffman, would injunctive relief in the courts be enough to change certain behaviors, do you think?

Ms. OYAMA. I think I just said courts do have the power of injunctive relief. I would want to echo the start businesses and start-up voices where they do say that the framework has created certainty, and that is essential for their content moderation and their economic viability.

Mr. SOTO. Thank you.

Mr. Huffman.

Mr. HUFFMAN. Similar answer, sir. I would shudder to think what would happen if we, when we were smaller, or even now, were on the receiving end of armies of tort lawyers.

Mr. SOTO. Ms. Citron, I see you nodding quite a bit. Injunctive relief, attorney's fees, are these things we should be looking at?

Ms. CITRON. So I just, as you say injunctive relief, all I can see is the First Amendment and prior restraint. So I think we need to be sort of careful the kinds of remedies that we think about. But law operates. If we allow law to operate, if people act unreasonably and recklessly, then I think the array of possibilities should be available.

Mr. SOTO. The last thing, I want to talk a little bit about 230, Section 230, as far as being incorporated in our trade deals. I am from Orlando, the land where a fictional mouse and a fictional wizard are two of our greatest assets.

Ms. Peters, I know you talked a little bit about the issue of including 230 in trade deals. How would that be problematic for a region like ours, where intellectual property is so critical?

Ms. PETERS. It is problematic because it potentially is going to tie Congress' hands from reforming the bill down the line, and that is precisely why industry is pushing to have it inside the trade deals.

Ms. OYAMA. There are 90 pages of copyright language in existing U.S. trade agreements. I think CDA 230 can just be treated the same if U.S. law doesn't bind Congress' hands at all.

Mr. SOTO. So if we adjusted laws here, that would affect the trade deals, is your opinion then?

Ms. OYAMA. There is no language in the trade deals that binds Congress' hands. Congress regularly has hearings on copyright, patent, pharmaceuticals, labor, climate, CDA 230. There is nothing in the trade agreement, the template language of U.S. law to create a U.S. framework when countries like China and Russia are developing their own frameworks for the internet, there is nothing in the current USMCA or the U.S.-Japan FTA that would limit your ability to later look at 230 and decide that it needs tweaks later on.

Mr. SOTO. Thanks. I yield back.

Ms. SCHAKOWSKY. The gentleman yields back, and that concludes our period for questioning.

And now I seek unanimous consent to put into the record a letter from Creative Future with attachments, a letter from American Hotel and Lodging Association, a letter from Consumer Technology Association, a letter from Travel Technology Association, a white paper from Airbnb, a letter from Common Sense Media, a letter from Computer & Communications Industry Association, a letter from Representative Ed Case, a letter in support of the PLAN Act, a letter from the i2Coalition, a letter to the FCC from Representative Gianforte, a letter from TechFreedom, a letter from the Internet Association, a letter from the Wikimedia Foundation, a letter from the Motion Picture Association, an article from The Verge titled "Searching for Help," a statement from R Street.

Without objection, so ordered.

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

Ms. SCHAKOWSKY. And let me thank our witnesses. I think this was a really useful hearing. I think those of you who have suggestions, more concrete ones than sometimes came up today, our committee would appreciate it very, very much. I am sure the joint committee would appreciate that as well, this joint hearing.

So I want to thank all of you so much for your thoughtful presentations and for the written testimony, which also often went way beyond what we were able to hear today.

And so I want to remind Members that, pursuant to committee rules, they have 10 business days to submit additional questions for the record to be answered by witnesses who have appeared.

And I want to ask witnesses to please respond promptly to any such questions that you may receive.

And at this time the committees are adjourned. Thank you.

[Whereupon, at 1:11 p.m., the subcommittees were adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. ANNA G. ESHOO

Chairman Doyle and Chairwoman Schakowsky, thank you for holding today's joint-subcommittee hearing, and thank you to each witness for testifying today. In particular, I welcome Ms. Katherine Oyama of Google, which is headquartered in my district, and Mr. Steve Huffman of Reddit, who joined me for a town hall meeting on net neutrality at Stanford University earlier this year. This important discussion is happening at a critical juncture in the development of the internet ecosystem.

Section 230 of the Communications Decency Act is the reason that the internet economy took off in the United States. It undergirds our ability to look up answers to questions, communicate with friends, stream videos, share photos, and so many other parts of our lives. As we discuss amending Section 230, we can't forget that it is a critical foundation for much of modern society.

I was a conferee for the Telecommunications Act of 1996, which included Section 230. I believed in the value of Section 230 then, and I believe in the importance of maintaining Section 230 now. I'm always open to debating how laws, including this one, can be improved, but I caution my colleagues to proceed very carefully in considering amendments to Section 230, since such a large part of our economy and society depends on it.

All of that being said, there are many issues with today's internet that could not have been conceived of in 1996. Congress can and should aim to solve these problems. The illegal sale of arms and opioids; radicalization of vulnerable individuals; planning mass violence; child sex abuse imagery; abuse and harassment of women and marginalized communities, especially through revenge pornography; deepfakes; misinformation, disinformation, and election interference; and doxxing and swatting are among the problematic practices that we should demand platforms moderate vigorously. When platforms fall short, we should consider making these acts violations of criminal law, to the degree that they are not already, before we view them through the lens of Section 230.

I look forward to a healthy and vigorous discussion to help inform our efforts to ensure that we have a healthy internet ecosystem that protects all users.

¹The CreativeFuture letter and attachments have been retained in committee files and also is available at <https://docs.house.gov/meetings/IF/IF16/20191016/110075/HHRG-116-IF16-20191016-SD005.pdf>.

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



U.S. House of Representatives Subcommittees on
Communications & Technology, Consumer Protection & Commerce

October 15, 2019

RE: NetChoice letter for the record for hearing: *Fostering a Healthier Internet to Protect Consumers*.

Dear Chairman Doyle and Chairwoman Schakowsky, Ranking Members Latta and McMorris Rodgers, and distinguished members of the Committee:

We thank the U.S. House of Representatives subcommittees on Communications & Technology, Consumer Protection & Commerce for holding this important hearing on *Fostering a Healthier Internet to Protect Consumers*.

NetChoice is a trade association of businesses who share the goal of promoting free speech and free enterprise on the net. We are significantly engaged in the states, in Washington, and in international internet governance organizations.

Today's hearing will demonstrate the fundamental need to retain Section 230 of the Communications Decency Act ("Section 230")¹ as it is written. Moreover, we hope that today's hearing will identify the failures of the prior edits to Section 230 (FOSTA)² and the harms that have resulted. Finally, today's hearing will hopefully identify the increasing need to promote America's values of free speech in other countries and how including such principles of Section 230 in our trade agreements will help bring free speech to other parts of the world.

It is important to remember the value of Section 230, not only to our free speech but to our economy. Section 230 enables a world-leading, innovative and competitive tech industry.

¹ 47 USC § 230.

² Pub. L. No. 115-164, 132 Stat. 1253 (2018).

Studies show³ that over the next decade, Section 230 will contribute a further 4.25 million jobs and \$440 billion in growth to the economy.

Section 230 has enabled the U.S. tech industry to far outperform the EU. In the U.S., online platform businesses are 5 times more likely to raise over \$10 million in venture capital funds than EU platform businesses.

In our letter for the record, we describe the origins and motivations for Section 230, clarify legal limitations of Section 230 in providing platform immunity for content created and posted by others, discuss the scope of what Section 230 does and does not allow, combat misinformation about Section 230 and outline the likely harms of amending Section 230.

History and purpose of Section 230

Section 230 was signed into law more than 20 years ago.⁴ When the law was conceptualized by Reps. Chris Cox (R-CA) and Ron Wyden (D-OR) in 1995, roughly 20 million American adults had access to the internet.

Those who took advantage of this opportunity, including many in Congress, quickly confronted this essential aspect of online activity: many users converge through one portal. The difference between newspapers and magazines, on the one hand, and the World Wide Web (as it was then called), on the other hand, was striking. In the print world, human beings reviewed and cataloged editorial content. On the Web, users created content which became accessible to others immediately. While the volume of users was only in the millions, not the billions as today, it was evident to almost every user of the Web that no group of human beings would ever be able to keep pace with the growth of content on the Web.

At the time, however, not all in Congress were users of the Web. The Communications Decency Act (“CDA”) was premised on the notion that the FBI could filter the web, screening out offensive content. This was a faulty premise based on a fundamental misunderstanding of the scale and the functioning of

³ Mike Masnick, *Don't Shoot the Message Board* (Aug. 2019).

⁴ 104 P.L. 104, 110 Stat. 56.

the internet. Nonetheless, in large part because the stated target of the CDA was pornography, the Senate voted overwhelmingly (the vote was 84-16) in favor of it.⁵

Section 230 was not part of the original Senate bill. Instead, it was introduced as the Internet Freedom and Family Empowerment Act in the House, which was intended *as an alternative to the CDA*. As is so often the case in legislative battles between House and Senate, the conferees on the Telecommunications Act of 1996, which became the vehicle for this subject matter, agreed to include both diametrically opposed bills. Subsequently, the U.S. Supreme Court gutted the CDA's indecency provisions, which it found violate of the First Amendment, giving Reps. Cox and Wyden an ultimate victory they did not at first win in conference.⁶

From the point of view of Section 230's authors, the fundamental flaw of the CDA was its misunderstanding of the internet as a medium. It was simply impracticable, they realized, for the bulletin boards, chat rooms, forums, and email that were then budding on the Web to be screened in any meaningful way by the operators of the websites and fledgling ISPs such as CompuServe and Prodigy that existed then. Worse, if the law were to demand such screening, the fundamental strength of the new medium – facilitating the free exchange of information among millions of users – would be lost.

The Prodigy and CompuServe cases

Then-Rep. Cox was on a flight from California to Washington, DC during a regular session of Congress in 1995 when he read a Wall Street Journal story about a New York Superior Court case⁷ that troubled him deeply. The case involved a bulletin board post on the Prodigy web service by an unknown user. The post said disparaging things about an investment bank. The bank filed suit for libel, but couldn't locate the individual who wrote the post. So instead, the bank sought damages from Prodigy, the site that hosted the bulletin board.⁸

Up until then, the courts had not permitted such claims for third-party liability. In 1991, a federal district court in New York held that CompuServe was not liable in circumstances like the Prodigy case. The court reasoned that CompuServe "had no opportunity to review the contents of the publication at

⁵ *Id.*

⁶ *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

⁷ Milo Geyelin, *New York judge rules Prodigy responsible for on-line content*, Wall St. Jo., May 26, 1995.

⁸ *Stratton Oakmont v. Prodigy Servs Co.*, 1995 WL 323710 (N.Y.Sup.Ct. May 24, 1995).

issue before it was uploaded into CompuServe's computer banks" and therefore was not subject to publisher liability for the third party content.⁹

But in the 1995 New York Superior Court case, the court distinguished the CompuServe precedent. The reason the court offered was that unlike CompuServe, Prodigy sought to impose general rules of civility on its message boards and in its forums. While Prodigy had even more users than CompuServe and thus even less ability to screen material on its system, the fact it announced such rules and occasionally enforced them was the judge's basis for subjecting it to liability that CompuServe didn't face.

The perverse incentive this case established was clear: any provider of interactive computer services should avoid even modest efforts to police its site. If the holding of the case didn't make this clear, the damage award did: Prodigy was held liable for \$200 million.¹⁰

By the time he landed in Washington, Rep. Cox had roughed out an outline for a bill to overturn the holding in the Prodigy case.

Creating Section 230 and its goals

The first person Rep. Cox turned to as a legislative partner on his proposed bill was Rep. Ron Wyden (D-OR). The two had previously agreed to seek out opportunities for bipartisan legislation. As this was a novel question of policy that had not hardened into partisan disagreement (as was too often the case with so many other issues), the two knew they could count on a fair consideration of the issues from their colleagues on both sides of the aisle.

For the better part of a year, the Congressmen conducted outreach and education on the challenging issues involved. In the process, they built not only overwhelming support, but a much deeper understanding of the unique aspects of the internet that require clear legal rules for it to function.

The rule established in their bill, which they called the Internet Freedom and Family Empowerment Act,¹¹ was pellucid: the government would impose liability on criminals and tortfeasors for wrongful conduct. It would not shift that liability to third parties, because to do so would directly interfere with the essential functioning of the internet.

⁹ *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 140 (S.D.N.Y. 1991) (emphasis added).

¹⁰ *Stratton Oakmont v. Prodigy Servs Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

¹¹ Internet Freedom and Family Empowerment Act, H.R. 1978, 104 Cong. (1995).

The Congressmen were well aware that whether a person is involved in criminal or tortious conduct is in every case a question of fact. Simply because one operates a website, for example, does not mean that he or she cannot be involved in lawbreaking. To the contrary, as the last two decades of experience have amply illustrated, the internet – like all other means of telecommunication and transportation – can be and often is used to facilitate illegal activity.

Section 230 was written, therefore, with a clear fact-based test.

- If one is a content creator, then one is liable for any illegality associated with that content.
- If one is not the content creator, then one is not so liable.

And what of the case where someone (or some company) is just partly involved in creating the content?

What if, moreover, they were only indirectly involved? In that case, Section 230 comes down hard on the side of law enforcement. In such cases, a website operator who is involved only in part, and only indirectly, is nonetheless deemed just as guilty as the content creator.

Here is the precise language of Section 230 in this respect:

The term “information content provider” means any person or entity that is responsible, in whole or *in part*, for the creation or *development of* information provided through the Internet¹²

At a recent forum in Washington, D.C., Rep. Cox, the lead drafter of Section 230, stated that these words in Section 230 – “in part” and “development of” – are the most important part of the statute.¹³

The clear intent of this plain language, and of Congress in enacting Section 230, was not to create immunity for criminal and tortious activity on the internet, but to ensure that innocent third parties will not be made liable for unlawful acts committed wholly by others. If an interactive computer service becomes complicit, in whole or in part, in the creation of illicit content – even if only by “developing” the content – then the service has no Section 230 protection.

This language in the statute proceeds directly from the legislators’ recognition that given the volume of content that passes through most internet portals, it is unreasonable for the law to presume that the

¹² 47 USC § 230(f) (emphasis added).

¹³ Armchair discussion with Former Congressman Cox, Back to the Future of Tech Policy, YouTube (August 10, 2017), https://www.youtube.com/watch?time_continue=248&v=iBEWXIn0JUY.

portal will screen all material. If in a specific case there is evidence that a portal did review material and edit it, then the plain language of Section 230 would deprive that portal of immunity.

Today, as federal and state law enforcement and civil litigants pursue Backpage.com, we have a clear example of how the law is designed to function. For purposes of analysis, let us assume the facts as they are presented in the Staff Report of the Senate Permanent Subcommittee on Investigations, “Backpage.com’s Knowing Facilitation of Online Sex Trafficking” (the “Senate Report”).¹⁴

Backpage, according to the Senate Report, systematically edits advertising for activity that is expressly made criminal under both federal and state law. Furthermore, Backpage proactively deletes incriminating words from sex ads prior to publication, to facilitate this illegal business while shielding it from the purview of investigators. Beyond this, Backpage moderators have manually deleted incriminating language that the company’s automatic filters missed. Moreover, Backpage coaches its users on how to post apparently “clean” ads for illegal transactions.

Furthermore, according to the Senate Report, Backpage knows that it facilitates prostitution and child sex-trafficking.¹⁵ It knows that its website is used for these purposes, and it assists users who are involved in sex-trafficking to post customized content for that purpose. Its actions are calculated to continue pursuing this business for profit, while evading law enforcement.

In sum, assuming these facts in the Senate Report are true, it is abundantly clear that Backpage is not a “mere conduit” of content created by others. The company is actively involved in concealing the illegal activity on its site by directly involving itself in modifying the content. This goes far beyond the minimum level of activity that eliminates immunity by Section 230’s standard of “indirect” involvement or mere “development” of content created by others.

Protecting the innocent and punishing the guilty

Throughout the history of the internet, Congress has sought to strike the right balance between opportunity and responsibility. Section 230 is such a balance – holding content creators liable for illegal activity while protecting internet platforms from liability for such content created entirely by others. At

¹⁴ Recognizing that the claims against Backpage.com are pending resolution in the courts, NetChoice does not by its assumption *arguendo* make any representation, express or implied, concerning the truth of the specific allegations in the Senate Report. NetChoice has no independent information concerning these specific allegations.

¹⁵ Staff Report at 37.

the same time, Section 230 holds platforms liable when they are complicit, even if only indirectly and even if only in part, in the development of illegal content.

The plain language of Section 230 makes clear its deference to criminal law. The entirety of federal criminal law enforcement is unaffected by Section 230. So is all of state law that is consistent with the policy of Section 230.¹⁶

Why did Congress not create a wholesale exemption of state criminal law, or state civil law, from the operation of Section 230?

First, and most fundamentally, it is because the essential purpose of Section 230 is to preempt state law like the court decision in *Prodigy*.¹⁷ Congress meant to establish a uniform federal policy, applicable across the internet, that would not punish an internet platform for the criminal or tortious conduct of another. Obviously, were state laws to be exempted from the coverage of Section 230, then Section 230 itself would become a nullity.

Even if such a wholesale exemption were limited to state criminal law, this would risk negating the federal policy. All a state would have to do to defeat the federal policy would be to place intermediary liability laws in its criminal code.

But in all other respects, Congress intended Section 230 to be entirely consistent with robust enforcement of state criminal law and state civil law. Today, every state and every federal prosecutor can successfully target online criminal activity by properly pleading that the defendant was at least partially involved in content creation, or at least the later development of it.

The importance of Section 230 for user-generated content

In simplest terms, Section 230 protects website operators that are not involved in content creation from liability for content or conduct by third party users. There is one exception to the rule that a website operator will become liable for “in part” developing content. If the website operator is involving itself in order to delete content that is “obscene, lewd, lascivious, filthy, excessively violent, harassing, or

¹⁶ 47 USC § 230(e)(3).

¹⁷ *Stratton Oakmont v. Prodigy Servs Co.*, 1995 WL 323710 (N.Y.Sup.Ct. May 24, 1995).

otherwise objectionable, whether or not such material is constitutionally protected,” then it is protected as a “Good Samaritan.”¹⁸

That liability protection has not only become the foundation supporting sites like eBay, Facebook, Amazon, Yelp, Twitter, and other well-known web brands that provide user-generated content (UGC), but also the entire Web 2.0 revolution through which thousands of smaller, innovative platforms have offered a range of socially useful services.

Without Section 230, small social media platforms would be exposed to liability for everything from users’ product reviews to book reviews. Airbnb would be exposed to liability for its users’ negative comments about a rented a home. Without Section 230, any service that connects buyers and sellers, workers and employers, content creators and a platform, victims and victims’ rights groups, or provides any other interactive engagement opportunity we can imagine, could not continue to function on the internet displaying user-generated content.

Coverage of Section 230

Some mistakenly claim that Section 230 prevents action against websites that knowingly engage in, solicit, or support criminal activity. As extensively discussed above, this is wrong. First, Section 230 expressly exempts violations of federal criminal law. Second, it bears repeating that Section 230 provides no protection for any website, user, or other person or business involved even indirectly in the creation or development of content that is tortious or criminal.

Why online sites and services cannot use Section 230 as a shield from federal prosecution

Section 230 provides online platforms no protection whatsoever from prosecution for violations of federal criminal law. Specifically, bad actors cannot rely on Section 230 as a shield from federal criminal prosecution because, by its express terms, Section 230 has no effect on federal criminal law. As noted above, Section 230(e)(1) clearly states:

No effect on criminal law - Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to

¹⁸ 47 U.S.C. § 230 (c)(2)(A).

obscenity) or 110 (relating to sexual exploitation of children) of title 18, *or any other Federal criminal statute*.¹⁹

As this is a matter of black-letter law, nothing more need be said on the point. The question, then, is whether existing federal criminal law suffices to prosecute offenses like terrorism and drug trafficking.

The answer is yes because there is a federal criminal proscription of terrorism²⁰ and drug trafficking.²¹

In all its actions to combat terrorism and drug trafficking on the internet under federal criminal law, Department of Justice will face no restrictions from Section 230.

Americans rely on Section 230 and oppose efforts to hold platforms liable

Americans, whether aware or not, rely on Section 230 every day.

Section 230 enables:

- Donations to charities via services like Donors Choose and GoFundMe.
- Finding babysitters via Care.com
- Helping to plan better vacations through review sites like Yelp and TripAdvisor.
- Learning new information from user-created content sites like Wikipedia.
- Discovering social issues via Change.org.

Tech platforms powered by Section 230 continuously protect consumers from harmful and illegal activity while empowering free speech online. The results from this polling showcase that maintaining Section 230 is a priority for the American people.

Polling by RealClear Opinion Research revealed that 62 percent of Americans say users who act illegally or post illegal content online are the ones who should be held responsible.

¹⁹ 47 U.S.C. § 230 (e)(1) (emphasis added).

²⁰ 18 U.S.C. § 113B.

²¹ 21 U.S.C. § 841.

Just 26 percent think the online platform should be held liable.

Section 230 enables online platforms to connect workers with potential employees, consumers to read reviews and comments to help them make decisions, and families to stay connected. It is understandable that the American public would continue to support Section 230 and not want to hold platforms liable for the content other people are posting.

Additional finds by RealClear Opinion Research found:

- Americans overwhelmingly (70%) say their ability to post or view user-created content online is valuable to their personal and professional lives.
- 62% of Americans say users who act illegally or post illegal content online are the ones who should be held liable.
- Of those polled, 73% say users, not platforms, should be held responsible for posts made in the comments section of a webpage.
- Only 1 in 5 polled say they trust the government keep online business practices ethical and fair, whereas a majority most trust consumers or businesses.

It's clear from this polling and activity that American consumers and voters have different priorities than the editors of legacy newspapers and broadcast media. Of course, legacy newspapers and broadcast media are actively stoking anti-tech sentiments with headlines that often blame social media for awful things that people do. It seems as if traditional media is consciously trying to defame social media in order to convince advertisers and audiences to come back to their websites and stations – not do what is best for Americans or do what Americans want.

Section 230 is the law that stops the spread of extremist speech

Throughout our discussions on Section 230, it's clear that some don't understand how fundamental Section 230 is in keeping our online interactions civil. That's not to say there aren't problems on the internet, but they are not as bad as they would be without Section 230. In fact, sites like 8-Chan, that engage in no content moderation, are least affected by removal of Section 230.

From our oped in Morning Consult:²²

There are those who wrongly say Section 230 is the reason for problems on the internet. They claim we would be better off without that law's incentives to moderate content created by users. These critics appear confused or disingenuous about what Section 230 actually does, and have apparently forgotten that our First Amendment says government cannot block hateful or disturbing speech — whether online or off.

Section 230 doesn't enable hate speech on the internet. It doesn't make the internet a worse place. It is actually the law that stands between an internet where much offensive content is removed and an internet where anything goes.

Despite the misinformation about the law, Section 230 actually has two components. The oft-cited "immunity provision" — Section 230(c)(1) — says that a platform is not liable for the content created by others, unless that content violates federal criminal or copyright law.

Despite what anti-tech advocates want you to believe, this is not a novel idea. This was Congress in 1996 enshrining what is called "conduit immunity," a legal concept that has been applied to all kinds of intermediaries since the 1950s — well before the creation of the internet.

Take for example Barnes & Noble. If it sells a book with libelous content, it would be absurd to hold Barnes & Noble liable. And if a criminal uses a phone to commit a crime, it would be absurd to hold AT&T liable. If you bought a lemon of a car listed in the NY Times classifieds, you could not hold the Times liable for misrepresentation in that ad.

Along comes the internet, and in 1991 a court applied this "conduit immunity" to an online message board that did no content moderation whatsoever. In essence, Section 230(c)(1) simply enshrined "conduit immunity" in law, but gave no platform immunity for violations of federal criminal or copyright law.

It is in the lesser-known Section 230(c)(2) that we see the real brilliance and benefit of this law at protecting us from hateful and extremist speech. Section 230(c)(2) empowers platforms "to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."

²² Carl Szabo, *Section 230 Is the Internet Law That Stops the Spread of Extremist and Hate Speech*, Morning Consult (Aug. 27, 2019).

Section 230(c)(2) enables Gmail to block spam without being sued by the spammers. It lets Facebook remove hate speech without being sued by the haters. And it allows Twitter to terminate extremist accounts without fear of being hauled into court. Section 230(c)(2) is what separates our mainstream social media platforms from the cesspools at the edge of the web.

Now let's suppose anti-tech advocates get their wish and upend Section 230. What would be the effect?

A diminished Section 230 makes it easier for hateful and extremist speech to spread to every corner of the internet. A diminished Section 230 makes it easier to send spam messages and viruses across the internet.

While some vile user content is posted on mainstream websites, what is often unreported is how much of this content is removed. In just six months, Facebook, Twitter, and YouTube took action on 11 million accounts for terrorist or hate speech. They moderated against 55 million accounts for pornographic content. And took action against 15 million accounts to protect children.

All of these actions to moderate harmful content were empowered by Section 230(c)(2).

Did Section 230 make the internet perfect? No. Nor did seat belts stop automobile fatalities. Is there room to improve the internet? Of course. But diminishing Section 230 will only make the internet worse, not better.

In essence, removing Section 230 will lead to the spread of more extremist speech.

Platforms actively engage in removing offensive and objectionable content

A report by NetChoice aggregated and clarified some of the findings and data from transparency reports by major social media platforms.

In just the six-months from July to December 2018, Facebook, Google, and Twitter took action on over 5 billion accounts and posts (5,051,079,936).

These takedowns over just six-months broke down in the following ways:

- Nearly 17 million accounts and posts removed related to Child Safety (17,243,426)
- Over 57 million accounts and posts removed related to Pornography and Nudity (57,300,867)
- Nearly 2 billion accounts and posts removed related to Fake Accounts, Impersonations, and Doxing (1,954,046,453)
- Over 3 billion accounts and posts removed related Spam (3,010,481,904)
- 12 million accounts and posts removed due to Extremist, Terrorist, and Hateful Conduct (12,007,286).

“Despite what you may hear, platforms are actively removing offensive and objectionable content all the time”

- Carl Szabo, Vice President
NetChoice


12 MILLION
extremism,
hate speech,
terrorism
REMOVED


2 BILLION
fake accounts,
impersonations,
doxing
REMOVED


17 MILLION
child safety
REMOVED


57 MILLION
nudity and
pornography
REMOVED

Failures and harms of prior amendments to Section 230

While some herald the passage of FOSTA as a success, such statements are questionable at best. In fact, new reporting shows that FOSTA has caused significant harms to local communities and resulted in increased police activity.

Since FOSTA’s enactment over a year ago, and despite the alleged benefits for law enforcement of FOSTA, we’ve actually seen a 25% *decrease* in prosecutions of sex-trafficking.²³ Moreover, we have unfortunately seen no evidence of significant decrease in sex-trafficking in the United States.

²³ Human Trafficking Institute, *2018 Federal Human Trafficking Report* (2018), available at <https://www.traffickingmatters.com/wp-content/uploads/2019/04/2018-Federal-Human-Trafficking-Report-Low-Res.pdf>.

As a result of the passage of FOSTA, cities like San Francisco have reported a 170% spike in sex-trafficking.²⁴

If there was a significant decrease in sex-trafficking, it would most likely be attributed to the takedown of Backpage.com. And while some mistakenly claim that the passage of FOSTA was necessary for the takedown of Backpage, the infamous website was removed before FOSTA was even signed into law calling into the underlying justification for FOSTA.²⁵

At the same time, even those groups who might have thought FOSTA was a good idea have realized that it is actually harming the efforts to help victims of sex-trafficking.²⁶

“ “[Passage of FOSTA] was unlike anything we’d ever seen,” says Meg Munoz, a sex-trafficking survivor and founder of the OC Umbrella Collective, an organization that serves sex workers and those being domestically trafficked in Southern California. “The immediate impact was swift and, honestly, terrifying. We watched people literally walk back to their pimps knowing they had lost any bit of autonomy they had. We watched people wind up homeless overnight. We watched members of our community disappear.”²⁷

...

“The legislators, law enforcement officials and advocates who championed SESTA and fought to take down Backpage, while perhaps well intentioned, have effectively forced an entire industry further underground, making the work of victim advocates and law enforcement that much more difficult.”

As predicted, the passage of FOSTA also unleashed frivolous civil lawsuits aimed at attacking deep-pocketed third-party businesses. *Doe v Salesforce* is part of a string of unintended consequences we’ve seen since the passage of FOSTA last year.²⁸

The plaintiffs assert that because Backpage.com used Salesforce’s tools (thousands of other sites use Salesforce’s tools as well), that Salesforce is directly liable for the harm caused by Backpage.com.

²⁴ CBS SF Bayarea, *New Laws Forced Sex Workers Back On SF Streets, Caused 170% Spike In Human Trafficking* (Feb. 3, 2019).

²⁵ *DOJ Seizes And Shuts Down Backpage.com (Before SESTA Has Even Been Signed)*, TechDirt (Apr. 6, 2018).

²⁶ *Anti-Sex-Trafficking Advocates Say New Law Cripples Efforts to Save Victims*, Rolling Stone Magazine (May 25, 2018).

²⁷ *Id.*

²⁸ More information at *DOE V SALESFORCE*, available at <https://netchoice.org/doe-v-salesforce-the-unintended-consequences-of-sesta-fosta/>.

Backpage.com, a notorious site where sex-trafficking occurred, was shut down by law enforcement in 2018 prior to the enactment of FOSTA.

While *Doe v Salesforce* does not specifically mention FOSTA or Section 230, it is clear that FOSTA potentially mollified Salesforce's ability to have the suit dismissed under Section 230.

Before the passage of FOSTA, Salesforce would likely have seen this suit immediately dismissed as a violation of Section 230 – which holds the bad actors, not the platforms responsible for violations of state law. But FOSTA opened holes in Section 230 allowing lawsuits like this one make the intermediary liable for abuses of their tools.

Moreover, FOSTA has afforded a cottage-industry for plaintiff's attorneys to grow and take action, not against bad actors, but instead deep-pocketed intermediaries like Salesforce. Note that the lead attorney in *Doe v Salesforce* is also the lead attorney in *Doe v Facebook* — both suits brought post-FOSTA enactment. It's very likely that these lawsuits are just the beginning of what is going to be a gold-rush for private attorneys.

So before we begin amending Section 230, we must look to see the effects of the prior actions – and clearly FOSTA has, unfortunately, failed to stymie sex-trafficking and has actually led to real harms for victims.

Importance of including Section 230 in trade agreements

Because of Section 230, U.S. companies, creators, and consumers have generated more free speech than at any time in the history of the world. For over 20 years, U.S. policy has encouraged user-created content on the internet.

Spreading free trade and free speech via inclusions of Section 230 in trade agreements

Section 230 enables greater free trade. A fundamental reason that platforms have been able to play a trade-enabling role is their open nature. Online services enable transactions and communications among millions of businesses and consumers, enabling US sellers to connect directly with global buyers. If there were a duty to inspect or filter each piece of content, then these services simply wouldn't exist, meaning that small businesses wouldn't be able to leverage new online tools to reach new customers abroad.

Over the next decade, Section 230 will contribute a further 4.25 million jobs and \$440 billion in growth to the economy.²⁹ And Section 230 has enabled the U.S. tech industry to far outperform the EU. In the U.S., online platform businesses are 5 times more likely to raise over \$10 million in venture capital funds than EU platform businesses. Section 230 enables a world-leading, innovative and competitive tech industry.

Research makes clear that Section 230 continues to enable strong American economic growth. There is a direct correlation between countries with intermediary liability protections like Section 230 and economic growth.

The fact that America, the birthplace of the internet, decided early on to “maximize user control over what information is received by individuals who use the Internet” established norms that should be emulated in countries around the world. The provisions in USMCA continue America’s goal of being a beacon to the world by encouraging adoption of Section 230 as a tool of democracy and free speech.

Section 230 has enabled speech from diverse political perspectives to flourish online in a way that never could have happened if just three networks or a handful of media companies were in a position to decide who can participate.

Addressing false claims by opponents of Section 230

While some special interests falsely claim that American does not add provisions to trade agreements that are currently being debated in Congress and agencies, this statement cannot be further from the truth.

Our trade agreements have often included provisions related to the protection of US copyrights and trademarks abroad. For example, the USMCA requires “a minimum copyright term of life of the author plus 70 years, and for those works with a copyright term that is not based on the life of a person, a minimum of 75 years after first authorized publication.” This provision is currently being debated in the halls of Congress as various interests are approaching life-end of their copyrights.

²⁹ Mike Masnick, *Don’t Shoot the Message Board* (Aug. 2019).

Likewise, USMCA includes provisions for protecting trademarks as legislatures and courts across the country are considering whether to amend our current trademark process like Trade Protection Not Troll Protection Act and cases being decided before US courts.

Also false are claims that including Section 230 in trade agreements will “tie the hands of congress.” Of course, we all know that unlike a treaty, the USMCA is only an agreement. This means that neither the US nor Mexico nor Canada are strictly bound to the text. In essence, if the US decides to exceed the text of the USMCA, it can.

Moreover, the power of Congress to exceed the text of the trade agreements is enshrined in the Trade Promotion Authority (reenacted in 2015). The TPA expressly included a section on “Sovereignty” to confirm that U.S. law has primacy over trade agreements.

Section 108(a) of TPA ensures that U.S. law will prevail in the event there is a conflict between the law and a trade agreement entered into under TPA. Section 108(b) ensures that no provision of a trade agreement entered into under TPA will prevent Congress from amending or modifying a U.S. law. Section 108(c) provides that dispute settlement reports issued under a trade agreement entered into under TPA shall have no binding effect on U.S. law.

Finally, USMCA is subject to longstanding exceptions that allow countries to enact measures “necessary for the protection of public morals.” USMCA negotiators made clear that this exception applies to Article 19.17, and highlighted the recent FOSTA-SESTA law as a recognized example under this exception.

In essence, arguments are **false** that say section 19.7 of the USMCA prevents Congress from amending Section 230 or that such inclusions are novel. Now is more important than ever to spread America’s values of free speech across the world and as such, now is the time to include platform immunities in our trade agreements.

Dangers of a “reasonableness” requirement for Section 230

Individuals like Danielle Citron mistakenly suggest that Section 230 require a reasonableness standard to hold platforms immune. This approach is flawed for many reasons.

A “reasonableness” standard will snowball legal costs for small platforms from \$80,00 to \$750,000 per suit.

As described above, the only sites and services that really need Section 230 are those that engage in content moderation. As shown through decades of case law, the immunity provision of Section 230 is not novel, and already exists in the form of “conduit immunity.” The need for Section 230 is for those platforms that engage in content moderation – like removal of extremist speech.

This means that only the platforms that seek to remove objectionable content need Section 230 – not sites like 8-Chan. Today, Section 230 provides these platforms an opportunity for a Fed. Civ. Law 12(b)(6) motion to dismiss (of course Section 230 has no effect on federal criminal actions as such law is exempted). Each time a site or service is sued, a motion to dismiss under Section 230 costs the site up to \$80,000.³⁰

Without this ability for a quick dismissal, these lawsuits can snowball to nearly \$750,000. For large platforms this may not be significant but imagine a smaller platform that faces just ten lawsuits – without Section 230, the small platform is looking at \$7.5million in legal fees. This is easily enough to put platforms out of business.

By a desire of small platforms to settle, even frivolous lawsuits, rather than suffer legal fees of \$750,000, this amendment of Section 230 will supercharge the plaintiff’s bar and ravage small entrepreneurs.

Conclusion

We thank the Committee for considering our views and we welcome the opportunity to provide more information about the importance of Section 230.

Sincerely,

Carl Szabo
Vice President and General Counsel, NetChoice
NetChoice is a trade association of online businesses. www.netchoice.org

³⁰ Engine, *Section 230: Cost Report*.

A World  **WITH or WITHOUT** Section 230

Section 230's Good Samaritan provision was enacted to empower platforms to moderate content without assuming liability for content posted by others.

Consumers want content moderation. Platforms without it can become venues for abuse, inappropriate content, and spam. Without content moderation, the world wide web would become the wild wild west.

There's a reason the most successful platforms all moderate user content.



With Section 230

Platforms could pursue good faith efforts to remove rule-breaking content, like pornography or drug use.

This is the heart of the Good Samaritan provision - don't punish good actors.

By empowering platforms to moderate content, platforms can protect their users from inappropriate content.

Section 230 encourages platforms to monitor content.

This empowers platforms to notify law enforcement when they observe criminal activity.

Moderation

Inappropriate Content

Illegal Content

Without Section 230

Without Section 230, platforms couldn't moderate without risking legal liability.

To avoid liability, platforms might not moderate at all.

Without Section 230, most online platforms would not risk engaging in removal of pornography and other inappropriate content.

Because platforms probably wouldn't moderate content, law enforcement would lose a valuable tool in stopping crimes and saving lives.

**Section 230 enables content moderation.
PROTECT SECTION 230. PROTECT OUR
ONLINE VOICES.**



Learn more at ProtectOnlineVoices.org

SECTION 230 MAKES ME A BETTER...

Neighbor



NextDoor.com makes it easier to keep in touch with my neighbors

Entrepreneur



Etsy and eBay help me grow my customer base

Citizen



Change.org enables me to get involved in local and national issues

Student



Wikipedia helps me research - even for controversial subjects

Traveler



TripAdvisor and Yelp help me plan better vacations and dining experiences

Donor



GoFundMe empowers me to help those I care about

Section 230 is federal law that lets these online platforms host and moderate user content - without risk of private lawsuits or liability for local laws.

If Yelp could be sued by restaurants over harsh reviews posted by users, Yelp would not be in business today.



Learn more at ProtectOnlineVoices.org

A day in the life of Section 230 on the hill



All platforms and services highlighted below would be impacted by changes to Section 230. Some would not be able to function, others would have to change their business model.

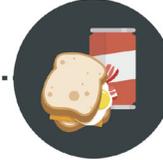
Section 230 enables user-generated content all over the web. Without it, the internet would not be what it is today.

AM



- Research for today's meetings using **Wikipedia**, **Google**, and **YouTube**
- Record public reaction to Rep's new op-ed on **Twitter**, **Facebook**, and **legacy newspaper comment sections**
- Reply to messages in my **email inbox**

LUNCH



- Find an event providing a free lunch for staffers on the hill using **Eventbrite**
- Look up **Yelp** reviews for tonight's happy hour location

PM



- Send out press statement on yesterday's big news **Facebook** and **Twitter**
- Research new contact on **LinkedIn** before you meet with them for coffee
- Post today's Rep remarks to our **YouTube channel!**

Section 230 enables user-generated content and provides us with the internet we use and rely on every day.

**PROTECT SECTION 230. PROTECT OUR
ONLINE VOICES.**



Learn more at ProtectOnlineVoices.org



Could Platform Safe Harbors Save the NAFTA Talks?

As the sixth round of talks over a modernized North American Free Trade Agreement (NAFTA) kicks off in Montreal, Canada, this week, EFF has joined with 15 other organizations and 39 academic experts to send the negotiators an [open letter](#) [PDF] about the importance of platform safe harbor rules, a topic that has been [proposed for the deal's Digital Trade chapter](#). The proposed rules, which are based on [S.47 U.S.C. section 230, a provision of the Communications Decency Act \("CDA 230"\)](#), would require that Internet intermediaries—whether giants like Facebook, or just your neighbour with an open Wi-Fi hotspot—[can't be held liable](#) for most speech of their users.

Usually our arguments for such strong platform safe harbor protections (which the letter refers to as intermediary immunity) center around how these support users' freedom of expression, by preventing would-be censors and critics from shutting down the platforms that host user speech. But as trade negotiators are not particularly receptive to [human rights arguments](#), instead our joint letter focuses on the economic arguments for platform safe harbors, which are also compelling:

First, intermediary immunity facilitates the development of effective reputation systems that strengthen markets. Reputation systems improve buyer trust and encourage vendors to compete on quality as well as price. Online, consumer review services and other wisdom-of-the-crowds feedback mechanisms have emerged that have no offline equivalent. However, online reputation systems require liability immunity to function properly. Otherwise, vendors can easily suppress truthful negative information via litigation threats. Immunity keeps that information online so that it can benefit consumers.

Second, intermediary immunity lowers the barriers to launch new online services predicated on third party content, making those markets more competitive. Without immunity, new entrants face business-ending liability exposure from day one; and they must make expensive upfront investments to mitigate that risk. Immunity lowers entrants' capital requirements and the riskiness of their investments, leading to more new entrants seeking to disrupt incumbents. This helps prevent the market from ossifying at a small number of incumbent giants.

The difficulty with the inclusion of Section 230 style safe harbors in NAFTA is that it would either require Canada and Mexico to change their law, or it would require the provision to be watered down in order to become compatible with their existing law—which would make its inclusion pointless. Therefore, the first option is the better one. For Canada, in particular, strengthening legal protection for Internet platforms could help roll back the precedent set in the [Google v. Equustek](#) case, in which the Canadian Supreme Court required Google to globally de-index a website that purportedly infringed Canadian trade secret rights.

Although changing Canadian law to strengthen platform safe harbors would be a significant step, there are certainly [even tougher issues](#) pending in the NAFTA negotiations, such as dispute resolution, government procurement, and America's demand for a five-year sunset clause. Moreover, Canada is asking a lot of the United States, too; having this month filed a broad-ranging [World Trade Organization \(WTO\) complaint](#) [PDF] against the United States alleging that the latter is flouting WTO rules in the way that it imposes tariffs and duties on other countries. In that context, reaching an agreement on platform safe harbors could become an olive branch to bring the countries closer to an overall deal.

Exporting Section 230 to Mexico and Canada isn't the only reason to advocate for its inclusion in a modernized NAFTA. This negotiation comes at a time when Section 230 stands under threat in the United States, currently from the [SESTA and FOSTA proposals](#), which could escalate into demands that platforms also assume greater responsibility for other types of content. As uncomfortable as we are with the lack of openness of trade negotiations, baking Section 230 into NAFTA may be the best opportunity we have to protect it domestically.

Officially, this is the second-last round of NAFTA talks that has been scheduled, although it seems next to impossible that the talks could be resolved in the next round. The two more likely scenarios are either that President Trump will notify the other parties that the U.S. is withdrawing from the existing NAFTA, or that

10/15/2019

Could Platform Safe Harbors Save the NAFTA Talks? | Electronic Frontier Foundation

additional rounds of negotiation will be scheduled after the Mexican general elections in July. Extending the negotiation would also leave more time for negotiators to begin to engage meaningfully with the public about platform safe harbors and other digital policy issues, which they have failed to do to date.

Frankly, we [don't think that trade agreements are the right place](#) to be negotiating rules for the Internet, and we'd rather that a Digital Trade chapter wasn't being negotiated at all, without significant reforms to the [transparency and openness of the negotiations](#). But if a Digital Trade chapter in NAFTA is inevitable, which seems to be the case, the better outcome for users is for broad platform safe harbor rules to be a part of that deal—both to protect users and innovators in the United States, and to ensure that the same level of protection applies North and South of the border.

JOIN EFF LISTS

Join Our Newsletter!

Email updates on news, actions, events in your area, and more.

Email Address

Postal Code (optional)

Anti-spam question: Enter the three-letter abbreviation for Electronic Frontier Foundation:

SUBMIT

RELATED UPDATES

Solutions for a Stalled NAFTA: Stop

<https://www.eff.org/deeplinks/2018/01/platform-safe-harbors-touted-safe-nafta-talks>

3/6



October 16, 2019

The Honorable Frank Pallone, Jr.
 Chairman, House Committee on Energy
 and Commerce
 2125 Rayburn House Office Building
 Washington, DC 20515

The Honorable Greg Walden
 Ranking Member, House Committee on Energy
 and Commerce
 2322 Rayburn House Office Building
 Washington, DC 20515

Dear Chairman Pallone and Ranking Member Walden:

On behalf of the American Hotel & Lodging Association (AHLA), the sole national association representing all segments of the U.S. lodging industry, including hotel owners, REITs, global brands, franchisees, management companies, independent properties, bed and breakfasts, state hotel associations, and industry suppliers, I would like to thank the House Committee on Energy and Commerce for holding today's hearing titled, "Fostering a Healthier Internet to Protect Consumers." As the Committee begins to review this important topic, AHLA encourages Congress to make clear that Section 230 of the federal Communications Decency Act (CDA 230) was not intended to stop state and local governments from putting in place rules and regulations governing short-term rentals in their communities.

The lodging industry is one of the nation's largest employers. Supporting 1 in 25 American jobs, or 8.3 million in total, the hotel industry annually provides more than \$92 billion in wages and salaries to our associates and generates \$660 billion in economic activity from the 5.3 million guestrooms at nearly 56,000 lodging properties nationwide. It's particularly important to note that this industry is comprised largely of small businesses, with nearly 60 percent of all hotels falling under the SBA's definition of what constitutes a small business in the lodging sector.

Passed in 1996, CDA 230 has played an important role in fostering the Internet's growth. CDA 230 provides Internet platforms with broad immunity from liability for third-party content posted on their websites. The original intent of CDA 230 was to shield an Internet company if users posted content that was obscene, lewd, excessively violent, or otherwise objectionable.

Unfortunately, today big tech short-term rental platforms, such as Airbnb and HomeAway, have exploited CDA 230 to avoid regulations and protect their profits. In fact, these companies have invoked the statute, arguing they are immune from regulations in at least 10 lawsuits against local governments across the country¹. In other words, these companies have used the statute to upend local ordinances governing short-term rentals, arguing that as "platforms" they cannot be forced to comply as they continue to profit from listings that violate local laws.

States and municipalities should be free to adopt and implement planning and zoning laws that govern short-term rentals. Multi-billion-dollar companies that profit from content on their websites should be accountable for that content and should be required to remove content advertising goods or services that are illegal offline. Congress should amend CDA 230 to make it clear that platforms are not immune from state and local laws holding them accountable for selling illegal products or services and make clear that massive technology companies such as Airbnb and HomeAway should abide by the same laws as every other law-abiding lodging business.

¹ Martineau, Paris. "Inside Airbnb's 'Guerrilla War' Against Local Governments." *Wired*. March 20, 2019. <https://www.wired.com/story/inside-airbnbs-guerrilla-war-against-local-governments/>



According to a recent national survey, Americans overwhelmingly support amending CDA 230 to remove loopholes used by short-term rental sites, like Airbnb and HomeAway, to avoid complying with state and local laws. Three in four Americans (76 percent) believe short-term rental sites should be held accountable for complying with local laws and 77 percent believe the CDA should be amended to remove potential loopholes, that allow Internet companies to profit off illegal activity on their web sites².

For these reasons, AHLA, along with a wide variety of local community interests strongly support the Protecting Local Authority and Neighborhoods (PLAN) Act (H.R. 4232)³. Introduced by Representatives Ed Case (HI-1) and Peter King (NY-2) and cosponsored by Representatives Norman (SC-5), Krishnamoorthi (IL-8), Dunn (FL-2) and Fitzpatrick (PA-1), the PLAN Act would amend CDA 230 to remove loopholes that short-term rental companies exploit to avoid compliance with local ordinances. This bipartisan legislation makes it clear that unlawful short-term rentals and illegal business transactions are not protected under federal law and Congress should act without delay.

Sincerely,

A handwritten signature in black ink that reads "Chip Rogers". The signature is fluid and cursive, with the first name "Chip" being more prominent than the last name "Rogers".

Chip Rogers
President and CEO

CC: Members of the House Committee on Energy and Commerce

² *Morning Consult*. "National Tracking Poll". August 27-29, 2019.

https://www.ahla.com/sites/default/files/morning_consult_survey_cda_short-term_rentals_9.10.2019.pdf

³ Riley, Tonya. "Airbnb now part of Congress's debate over Silicon Valley's legal shield." *Washington Post*. October 14, 2019. <https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/10/14/the-technology-202-airbnb-now-part-of-congress-s-debate-over-silicon-valley-s-legal-shield/5da3b24f8e0fa3155a710c2/>



1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

The Hon. Frank Pallone
Chair, Energy and Commerce Committee

The Hon. Greg Walden
Ranking Member, Energy and Commerce Committee

The Hon. Mike Doyle,
Chair, Communications and Technology Subcommittee

The Hon. Robert E. Latta
Ranking Member, Communications and Technology Subcommittee

The Hon. Jan Schakowsky
Chair, Consumer Protection and Commerce Subcommittee

The Hon. Cathy McMorris Rodgers
Ranking Member, Consumer Protection and Commerce Subcommittee

Dear Reps. Pallone, Walden, Doyle, Latta, Schakowsky and McMorris Rodgers:

Before your hearing on Section 230 of the Communications Decency Act and online content moderation, we ask you to consider the Consumer Technology Association's (CTA) views on Section 230 and its unique role in fueling American innovation.

Section 230 establishes the common-sense principle that responsibility for online speech lies with the speaker, not the platform. Equally important, Section 230 enables online platforms to remove offensive, obscene or hateful content without liability.

Section 230 does not provide legal immunity for sites hosting copyright-infringing material, nor does it provide protection for platforms violating federal criminal law.

The U.S. approach to online speech regulation has allowed American innovation to thrive. This approach is largely responsible for U.S. global online leadership, as well as our country's unique and dynamic startup economy. Because of Section 230, U.S. businesses are the global default choice for finance, communication and entertainment. Section 230 is so important that author and professor Jeffrey Kosseff termed the provision "the twenty-six words that created the Internet."





1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

Internet platforms hosting third-party speech relying on Section 230 include job search sites, home-sharing platforms, social networks, online classified ads, cloud storage companies, podcast distributors, digital marketplaces and all newspapers or online publications with a comment section. Together, these platforms make up a major part of the daily Internet experience enjoyed by millions of Americans.

Without Section 230 protections, these platforms could face massive potential legal liability for any third-party post. Online sites would be barraged with litigation (frivolous and otherwise) from those angry with views expressed on the platform or those unhappy that their content has been taken down.

As a result, online platforms would be forced to over-moderate and take down speech that, while lawful, is also controversial or could conceivably lead to a lawsuit. As a result, the Internet would lose much of its vitality and usefulness as a platform for discussion and commerce.

While the Section 230 discussion often revolves around large Internet companies, these protections are most vital for small businesses and startups that do not have large legal departments or litigation budgets. In a non-Section 230 world, any startup hosting third party speech could face costly lawsuits from all corners of the Internet. Venture capitalists would be dissuaded from investing, and new competitors and market entrants would never get off the ground. America's uniquely vibrant Internet startup ecosystem is a direct result of the protections offered by Section 230.

Given Section 230's benefits to U.S. innovation, it is entirely appropriate that similar language be included in the United States–Mexico–Canada Agreement (USMCA) and other trade agreements. These trade agreement provisions ensure that U.S. businesses can continue to expand beyond our borders without foreign governments imposing new restrictions that could never be tolerated. More, the provisions promote key American values by discouraging our trading partners from unduly restricting online free expression and creating a totalitarian-style Internet. Finally, intermediary liability provisions in trade agreements reassure American small businesses seeking to participate in international markets that they will not be held liable for user-created speech, such as customer reviews.

It is ironic that while competitors like China are spending billions to catch up with American technology companies, some in Congress are contemplating dismantling the very legal structure that makes our leadership possible. This discussion is being encouraged by a variety of legacy industries unhappy with new and popular online competitors. U.S. policy should not be driven to protect incumbent business interests, models or hegemonies.





1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

I urge your committees not to weaken our innovation economy and global technology leadership. Instead, I implore you to protect America's startups and entrepreneurs by safeguarding and preserving Section 230.

Sincerely,

A handwritten signature in black ink, appearing to read "M Petricone".

Michael Petricone
Senior Vice President
Consumer Technology Association

cc: Members of the Subcommittee on Communications and Technology
Members of the Subcommittee on Consumer Protection and Commerce



What Others are Saying About Section 230

“Even if today’s internet giants can survive the loss of Section 230 and absorb the costs of censorship compliance, new market entrants likely can’t. Which means that hobbling 230 will stifle the competition that got us to today’s rich internet in the first place.”

- R Street Institute

“The legal protections provided by CDA 230 are unique to U.S. law...most prominent online services are based in the United States. This is in part because CDA 230 makes the U.S. a safe haven for websites that want to provide a platform for controversial or political speech and a legal environment favorable to free expression.”

- Electronic Frontier Foundation

“Given the staggering scale and breathtaking speed at which users post content online, there’s just no way for social networks to vet content the way newspapers vet letters to the editor. This makes Section 230’s shield against liability for user-generated content as essential to social networks as a broadcast license was for broadcasters.

- Tech Freedom

“Section 230 creates the breathing room not only for direct competitors to today’s dominant sites for user-generated content, but also for the development of completely alternative models for interactive online services.”

- Center for Democracy and Technology

“Section 230 does not protect only the large firms such as Facebook and Google, but rather continues to provide liability protection for large and small distributors alike... Congress recognized, as the courts had in several First Amendment cases for traditional media, that publisher and republisher liability chills the free exchange of controversial ideas and criticism.”

- Mercatus Center

“The Internet flourishes when social media platforms allow for discourse and debate without fear of a tidal wave of liability. Ending Section 230 would shutter this marketplace of ideas at tremendous cost.”

- Taxpayers Protection Alliance

Section 230 provides companies with a safe harbor to do what Congress cannot do under the First Amendment: decide to take down content that is offensive or otherwise not wanted on their platforms. Imposing liability on companies for their users’ content will incentivize platforms to err on the side of censorship and threaten free expression online.”

- New America’s Open Technology Institute



September 9, 2019

The Honorable Frank Pallone
Chairman
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Greg Walden
Ranking Member
House Committee on Energy & Commerce
2322-A Rayburn House Office Building
Washington, D.C. 20515

The Honorable Michael F. Doyle
Chairman
House Subcommittee on Communications
& Technology
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Robert E. Latta
Ranking Member
House Subcommittee on Communications
& Technology
2322-A Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Pallone, Ranking Member Walden, Chairman Doyle, and Ranking Member Latta:

The Travel Technology Association (Travel Tech) opposes the *Protecting Local Authority and Neighborhoods (PLAN) Act of 2019*, a bill that would weaken a crucial internet law while unfairly targeting short-term rental platforms for the sole purpose of limiting competition for the hotel industry.

Section 230 of the Communications Decency Act (CDA) has been enormously important to the growth of the internet by providing legal certainty to an ever-expanding world of internet services, including social media, blogs, consumer review sites, search engines, and in the case of our members, travel and accommodations intermediaries and platforms. This legal standard has provided an environment that promotes innovation and has allowed the internet to grow and thrive over the past two decades. Absent the protections of Section 230, all internet platforms would be obligated to police and censor content under the threat of massive legal liability, destabilizing the internet as we know it, and opening up companies to endless frivolous lawsuits.

The PLAN Act would carelessly amend Section 230 by removing the preemption for user-generated content only in cases of online short-term rentals. While recent traveler trends have fostered a new generation of vacation rental travelers, platforms have also stepped up to offer innovative solutions to local concerns. Short-term rental platforms are working with municipalities every day to find reasonable and effective solutions to increase compliance, address non-compliance, and foster a short-term rental environment that works for the entire community. In fact, in many cities across America (Chicago, for example), short-term rental platforms have agreements with the city that allow platforms to share data in a way that enables the city to accomplish everything it wants without Congress having to remove critical Section 230 protections.

To take such a bold step of amending the CDA in this way, which has stood the test of time and maintains a reasonable standard for e-commerce, is completely unnecessary,

will not address any perceived problems associated with the short-term rental industry, and is just another attempt by a special interest to stifle innovation by destroying a core underpinning of the internet.

Any further amending of Section 230 of the CDA must be carefully and thoughtfully considered, not cheapened by special interests looking to secure an advantage over their perceived competition in the marketplace. I appreciate this opportunity to share our industry's perspective on the PLAN Act, and urge you and your colleagues on the committee to reject it outright.

Sincerely,

A handwritten signature in black ink, appearing to read "Steve Shur". The signature is fluid and cursive, with a large initial "S".

Steve Shur
President
The Travel Technology Association



Airbnb & the Communications Decency Act Section 230

For over 20 years, the Communications Decency Act's Section 230 (CDA230) has served as the legal underpinning that allows user-generated content to flourish on the internet. CDA230 fosters a free and open internet by shielding online intermediaries ("interactive computer service providers") from being treated as the publisher or speaker of content authored by a third party. CDA230 encourages online intermediaries to engage in content moderation such as screening, reviewing, editing, and blocking content, without fear that their good faith efforts will expose them to liability -- without this protection, online intermediaries would be adversely incentivized to censor constitutionally protected speech to avoid potential lawsuits.

Ensuring users' safety and enhancing their experience. There have been 500 million guest arrivals all-time through Airbnb's trusted accommodation marketplace, and on the average night there are 2 million people staying on Airbnb. Because of CDA230, Airbnb is able to screen content, use editorial discretion, and block objectionable material to ensure smooth stays for both hosts and guests. For example CDA230 protections enable us to:

- *Provide User Reviews:* After each stay, our two-way blind review system prompts guests and hosts to review each other. This ensures honest feedback and increases trust in the community and the experiences provided by hosts. We currently have a robust [content policy](#) to allow for this trustworthy review system while ensuring Airbnb can filter and take down objectionable content. A recent Internet Association survey¹ shows that two thirds of Americans check online reviews almost every time they buy online or visit a business, and they trust those reviews to give an accurate impression. And 82% of respondents say user reviews make them feel more safe when booking a short-term rental online.
- *Ensure User Safety:* The safety of our community is our priority and to that end, Airbnb has strong [Community Standards](#) to ensure safety and foster belonging. Because of Airbnb's content moderation activity in this area, we are able to monitor and take down objectionable content on issues ranging from spam, to threats of harm, intellectual property, harassment, authenticity, and quality control/reliability.
- *Prevent Discrimination:* Our [Non-Discrimination Policy](#) allows for everyone in our community to feel welcome and respected, and it allows for Airbnb to review and take down discriminatory content and hate speech.

Maintaining a Competitive Marketplace for All Consumers. Airbnb leverages technology to provide access to more than 7 million unique places to stay in more than 100,000 cities and 191 countries and regions. These listings are offered by our users, who describe the listing, how much to charge, and how often to rent it. As a result, Airbnb not only helps individuals generate supplemental income through STRs, but it also empowers consumers with a wide variety of choices for short-term accommodations at all price points.

¹ The Best Of The Internet survey was conducted via online interviews through SurveyMonkey from May 21-22. The survey included interviews with 2451 American Adults. Topline results are available [here](#).



Each of the 100,000 cities where hosts post Airbnb listings has their own needs and priorities for STR rules in their community. Airbnb works with cities worldwide on sustainable, scalable, and reasonable solutions to help jurisdictions curtail bad actors and enforce their laws. Throughout the United States, Airbnb has worked with cities to develop more than 500 partnerships including fair, reasonable regulations, tax collection agreements, and data sharing that balance the needs of communities. This allows hosts the opportunity to share their homes in order to pay the bills and guests the opportunity to find affordable accommodations from big cities to small towns in every corner of the country.

Airbnb's Terms of Service and [Responsible Hosting Pages](#) inform hosts about the importance of being a good neighbor and understanding local laws. We also engage with our host community through educational workshops and communications regarding their local laws. And we partner with cities to implement tools that facilitate enforcement of their laws. **However, it would be unsustainable for Airbnb to be responsible for monitoring more than 7 million listings worldwide for their compliance with the thousands of individual local laws aimed at host-generated content.**

Simply put, the protections of CDA230 make it possible for Airbnb to operate our marketplace for hosts and guests, working with cities to curtail bad actors without taking on unreasonable and cost-prohibitive legal liability for all of the millions of pieces of user-generated content on the platform.



October 15, 2019

Honorable Frank Pallone
 Chairman, Energy and Commerce
 2125 Rayburn House Office Building
 Washington, D.C. 20515

Honorable Greg Walden
 Ranking Member, Energy and Commerce
 2322 Rayburn House Office Building
 Washington, D.C. 2051

Re: Statement of James P. Steyer, CEO and Founder of Common Sense Media regarding the Hearing on Sec. 230 and "Fostering a Healthier Internet to Protect Consumers."

Dear Chairman Pallone and Ranking Member Walden:

Thank you for the opportunity to submit this comment for the record on your important hearing on Sec. 230 and "Fostering a Healthier Internet to Protect Consumers." I am grateful that you are taking up this pressing issue that affects our country and our democracy and that also directly impacts kids and families, and I hope that you will closely consider the unique needs of children as you explore the issues surrounding Sec. 230 and the proliferation of harmful content online.

Common Sense Media is America's leading organization dedicated to helping kids and families harness the power of media and technology as a positive force in kids' lives. We have a deep background in telecommunications policy as it relates to kids and families. Launched 15 years ago, Common Sense Media has more than 110 million unique consumer users each year. We provide independent research, advice, ratings and reviews, and trustworthy information to help families thrive in the 21st century. s technology products are now an integral part of the school experience, we designed an award-winning Digital Citizenship Curriculum to help educators with a comprehensive K-12 curriculum that guides students through technology dilemmas (cyberbullying, tech addiction, and news literacy, for example). More than 700,000 registered educators use our resources and we have more than 68,000 member schools, including well over half of U.S. schools and 14,000 schools in other countries. Through our Common Sense Research program, we provide provide parents, educators, health organizations, and policymakers with reliable, independent data on children's use of media and technology and the impact it has on their physical, emotional, social, and intellectual development. Common Sense has been an important voice in Congress, before the FCC and FTC, and in state legislatures regarding children's online privacy and digital equity issues.

I am deeply concerned that Sec. 230 has allowed for an explosion of irresponsible, harmful, and dangerous content on the Internet with no accountability for the companies that house and profit off that content. It is my view that without a strong government incentive, industry efforts to take down or limit harmful content are often inadequate reactive "one-offs." Platforms promise a safe environment for friends and families to

connect and share but industry's own "community standards" are not reliable and result in parents being left with the overwhelming challenge of trying to "moderate" the internet for their kids on their own. Platforms could design their sites to support content moderation and to guide kids and parents to healthy content but instead parents are contending with both dangerous content and manipulative design techniques that relentlessly push content and addictive use. Technology companies can and should step up but the current language and interpretations of Sec. 230 have allowed companies to abdicate this duty.

While more longitudinal research is needed on the impact our "always on" culture is having on our kids, what we do know, and what many parents have experienced firsthand, is that there has been rapid growth in the last few years when it comes to access to technology and the amount of time kids and families spend in front of screens. In 2012, 34 percent of teens used social media more than once a day; today, 70 percent do.¹ At the same time, most teens -- seventy-three percent -- think social media is designed to make them spend more time on their devices and distract them and their friends. Notably both kids and parents share concerns about the content they come across on platforms.

Here are some of the things we already know about digital media consumption that are relevant to the debate over Sec. 230 as highlighted by MacArthur Genius Award Recipient and legal scholar, Danielle Citron, in "[The Internet's Safe Harbor is Not Safe for Kids](#)"²:

Kids of all ages are watching -

- Eighty-one percent of parents with children 11 and younger let their kids watch videos on YouTube.³
 - Sixty-one percent of these parents say their child has encountered content on YouTube that they felt was unsuitable for children.⁴
- Eighty-five percent of teens say they use YouTube.⁵
- Teens use Instagram (61%), Snapchat (63%), and Facebook (43%).⁶

¹ Rideout, V., & Robb, M. B. (2018). *Social media, social life: Teens reveal their experiences*. San Francisco, CA: Common Sense Media.

² <https://www.common Sense Media.org/kids-action/blog/the-internets-safe-harbor-is-not-safe-for-kids>

³ Smith, A., Toor, S., & Van Kessel, P. (2018, November 7). *Many turn to YouTube for children's content, news, how-to lessons*. Retrieved from

<https://www.pewinternet.org/2018/11/07/many-turn-to-youtube-for-childrens-content-news-how-to-less-ons/>.

⁴ *Id.*

⁵ Pew Research Center (2018, May). *Teens, social media & technology*. Retrieved from <https://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/>

⁶ <https://www.common Sense Media.org/research/social-media-social-life-2018>

Vulnerable teens feel more vulnerable online -

- Teens with low social-emotional well-being experience more of the negative effects of social media than kids with high social-emotional well-being.⁷

Teens are on social media more than ever -

- The proportion of teens who use social media multiple times a day has doubled over the past six years: In 2012, 34% of teens used social media more than once a day; today, 70% do.⁸

Kids use social media as a source for news -

- Among children aged 10 to 18 who use social media, 76% get news from a social networking site. Of those:⁹
 - Forty-one percent of tweens choose YouTube as their preferred social media site for news.¹⁰
 - Forty-seven percent of teens choose Facebook as their preferred social media site for news.¹¹

Social media is cause for concern -

- Fifty-four percent of teens say that if parents knew what actually happened on social media, they'd be a lot more worried about it.

Because most platforms turn a profit from advertising revenue, the incentives for a platform to “self regulate” and use the “sword” to moderate content as Sec. 230 intended are misaligned with a platform’s own needs to turn that profit. Platform ad revenue depends on driving traffic to the site and keeping users on the site. The easiest way to do this is by allowing for the most outrageous content to proliferate. Platforms then push that outrageous content to kids (recommendation algorithms) and employ manipulative design techniques (autoplay, likes, streaks, badges) to keep kids on the platform. Instead of managing content as the authors of Sec. 230 envisioned, platforms see Sec. 230 as a simple “shield” to protect them from the liability that could arise from all the harmful, toxic, extreme, and even illegal material they allow on their sites. Pushing this toxic content is a simple path to profits and Sec. 230 neutralizes any outside incentives that might have lead these companies to moderate their platforms.

Amending Sec. 230, admittedly a difficult endeavor, is necessary to ensure a safer online environment for children. We must ensure that the language of Sec 230 both allows for platforms to moderate content but also to incentivize that platforms *actually* moderate

⁷ Rideout, V., & Robb, M. B. (2018). *Social media, social life: Teens reveal their experiences*. San Francisco, CA: Common Sense Media.

⁸ Rideout, V., & Robb, M. B. (2018). *Social media, social life: Teens reveal their experiences*. San Francisco, CA: Common Sense Media.

⁹ <https://www.common sense media.org/research/news-and-americas-kids-infographic>

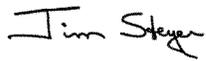
¹⁰ *Id.*

¹¹ *Id.*

content. Today, kids must be online for life and learning, platforms and government have a responsibility to make sure there are safeguards in place.

Thank you for your consideration of these comments as you debate the best path forward regarding Sec. 230 and ensuring the Internet is a safe place for everyone. Common Sense stands ready to assist you as you move ahead on this important issue.

Sincerely,

A handwritten signature in black ink that reads "Jim Steyer". The signature is written in a cursive, slightly slanted style.

James P. Steyer
Founder and CEO, Common Sense



October 15, 2019

The Honorable Frank Pallone
Chairman
House Energy and Commerce Committee
Washington, DC 20515

The Honorable Greg Walden
Ranking Member
House Energy and Commerce Committee
Washington, DC 20515

The Honorable Richard Neal
Chairman
House Ways and Means Committee
Washington, DC 20515

The Honorable Kevin Brady
Ranking Member
House Ways and Means Committee
Washington, DC 20515

The Honorable Chuck Grassley
Chairman
Senate Finance Committee
Washington, DC 20510

The Honorable Ron Wyden
Ranking Member
Senate Finance Committee
Washington, DC 20510

Re: Importance of Intermediary Protections to U.S. Exports

Dear Chairman Pallone, Chairman Neal, Chairman Grassley, Ranking Member Walden, Ranking Member Brady, and Ranking Member Wyden:

Our organizations represent a wide range of companies and organizations that depend upon intermediary protections such as Section 230 of the Communications Decency Act to grow in the United States and export to markets around the world. Section 230 facilitates legal online commerce and communication, allowing millions of entrepreneurs, small businesses, and diverse voices to flourish.

The U.S. legal framework for online platforms is critical to American leadership in digital trade, including our \$172 billion digital trade surplus.¹ This framework enables growth and innovation across the creative and technology sectors, while enabling small U.S. businesses and startups to scale up quickly and become exporters. Undermining foundational intermediary liability protections would cost 4.25 million American jobs and \$400 billion over the next decade, according to recent research.²

Unfortunately, threats to this framework are mounting globally, and American leadership on this issue has become increasingly critical. Countries such as China, Russia, India, and parts of the European Union have pursued a very different approach through legal regimes that require state control of online speech, activity and commerce. These countries are actively pushing some of our key trading partners to adopt similar penalties and seek to apply their rules in an extraterritorial way that restricts market access for U.S. firms.

¹ Bureau of Econ. Affairs, U.S. Trade in ICT and Potentially ICT-Enabled Services (last updated Oct. 19, 2018).

² Christian Dippon, *Economic Value of Internet Intermediaries and the Role of Liability Protections* (NERA 2017), <http://internetassociation.org/wp-content/uploads/2017/06/Economic-Value-of-Internet-Intermediaries-the-Role-of-Liability-Protections.pdf>.

If the U.S. were to abandon its leadership position on this issue, it would send a clear signal to these and other countries that they are free to pursue further troubling restrictions on speech and innovation. Stakeholders broadly recognize the need for a robust system of intermediary liability protections, while still providing for healthy debate on the exact contours of Section 230.³

Promoting intermediary liability protections in a trade agreement serves several key functions. It stops foreign restrictions on free expression and innovation, and it gives companies the legal certainty they need to take “Good Samaritan” steps to proactively remove abusive and malicious content from their platforms. The Good Samaritan provisions in Section 230 are designed to enable website operators to fight misconduct and protect their users from online harms by removing disincentives to moderate abusive behavior. Narrowing this protection would have the perverse result of making it harder for website operators to police bad actors.

Intermediary liability protections also play a key role in enabling American small businesses to build trust and customer relationships in new markets. Today, millions of U.S. small businesses are taking advantage of online commerce to reach far beyond local markets, including through marketing tools and interactive customer services. However, for these trade-enabling tools to function, companies need legal certainty that they will not be held liable for all communications that arise between businesses and consumers using these tools. The inclusion of intermediary protections in trade agreements provides this assurance. As the U.S. International Trade Commission recently recognized, “provisions that reduce policy uncertainty about digital trade” are one of the most economically significant elements of the USMCA.

Finally, some have raised the concern that a trade agreement somehow ‘locks in’ domestic law. The protections in trade agreements, like U.S. law, provide clear flexibility for domestic changes to legal frameworks. In the U.S., criminal law is explicitly exempt from the law to ensure prosecution of bad actors. In the general exceptions to USMCA and other trade agreements, there is an exemption allowing for new laws to protect public morals and other interests. USMCA shows how trade measures can be sufficiently flexible to reflect new changes to a legal framework.

Thank you for your attention to this issue. We look forward to collaborating with you further to strengthen the American approach to digital trade on which so many of our nation’s creators, inventors, consumers, and businesses depend.

Sincerely,

Computer & Communications Industry Association
Consumer Technology Association
Engine
Internet Association
NetChoice

³ Chamber of Commerce *et al.*, 27-Association Global Industry Position Paper on WTO E-Commerce Initiative, Oct. 7, 2019, <https://www.iftc.org/dotAsset/f2de6c22-e286-47d2-aca7-ba34830e462c.pdf>

ED CASE
1ST DISTRICT, HAWAII

2443 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
TELEPHONE: 202-225-2726
FAX: 202-225-0688

1132 BISHOP STREET, SUITE 1910
HONOLULU, HI 96813
TELEPHONE: 808-650-6688
FAX: 808-533-0133

WEBSITE: CASE.HOUSE.GOV

Congress of the United States
House of Representatives
Washington, DC 20515

COMMITTEE ON APPROPRIATIONS
SUBCOMMITTEES:
MILITARY CONSTRUCTION, VETERANS AFFAIRS
AND RELATED AGENCIES

COMMERCE, JUSTICE, SCIENCE AND RELATED
AGENCIES

LEGISLATIVE BRANCH

COMMITTEE ON NATURAL
RESOURCES
SUBCOMMITTEES:
NATIONAL PARKS, FORESTS AND PUBLIC LANDS

WATER, OCEANS AND WILDLIFE

INDIGENOUS PEOPLES OF THE UNITED STATES

October 16, 2019

The Honorable Michael F. Doyle
Chair
Subcommittee on Communications and
Technology
House Committee on Energy and Commerce
2123 Rayburn House Office Building
Washington, DC 20515

The Honorable Robert E. Latta
Ranking Member
Subcommittee on Communications and
Technology
House Committee on Energy and Commerce
2123 Rayburn House Office Building
Washington, DC 20515

The Honorable Janice D. Schakowsky
Chair
Subcommittee on Consumer Protection and
Commerce
House Committee on Energy and Commerce
2123 Rayburn House Office Building
Washington, DC 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
Subcommittee on Consumer Protection and
Commerce
House Committee on Energy and Commerce
2123 Rayburn House Office Building
Washington, DC 20515

Dear Chair Doyle, Chair Schakowsky, Ranking Member Latta and Ranking Member McMorris Rodgers,

Thank you for holding this important joint subcommittee hearing, "Fostering a Healthier Internet to Protect Consumers," to review the impact of websites' content moderation efforts and Section 230 of the Communications Decency Act (CDA 230).

There is a broad array of issues that this hearing will cover as the internet has become such a dominant force and pervasive influence in our society. However, I want to bring specific attention to one aspect that arises out illegal short-term or vacation rentals that have become a major concern for communities across the country.

Last month, I introduced H.R.4232, the Protecting Local Authority and Neighborhoods (PLAN) Act, which would end abusive litigation by internet-based short-term rental platforms attempting to avoid accountability for profiting from illegal rentals and strike down local regulations aimed at curbing this illegal activity and its widespread negative impacts. These impacts include

unavailability of affordable housing, avoidance of standard consumer protections and loss of state and local government revenue. The bill is bipartisan and has a geographically diverse group of cosponsors.

Over the past decade-plus, the short-term vacation rental industry has exploded through the internet-based marketing platforms of Airbnb, HomeAway, VRBO, Flipkey and others. While some communities welcome this activity, which is largely conducted in residential neighborhoods, many others are concerned with several negative consequences.

These include the loss of affordable housing as residential units are converted to transient accommodations for tourists, and the failure of many unit owners and rental operators to comply with basic consumer safety, public accommodations and tax requirements as must the legal lodging industry. A survey of related news also makes clear that commercial lodging activity in otherwise residential neighborhoods gives rise to serious community safety and disruption issues. Attached is a letter from community advocates outlining concerns about how the short-term rental market being facilitated by online platforms have directly impacted housing affordability.

As a result of the impacts of the explosion of short-term rentals, from Hawai'i to Maine state and local governments are updating their land use laws to put parameters around short-term rental activity, tailored to reflect local concerns and as always has been the case with land use regulation. However, the short-term rental online platforms have repeatedly gone to court to strike down these laws, claiming CDA 230 preempts local efforts to stop the listing and booking of illegal rentals by these platforms. They have sued cities large and small – including New York City, Boston, Miami, Anaheim, San Francisco, Portland, Ore., Chicago, Miami Beach, Palm Beach and Santa Monica – to protect a business model they know relies in large part on concealing the illegal activity of their third-party operators.

The PLAN Act would amend CDA 230 to make clear the statute does not shield platforms when they facilitate illegal rental bookings. Platforms would also be accountable if they fail to stop booking rentals after receiving notice from a private property owner that short-term rentals are prohibited at that location. This leaves zoning ordinances and enforcement to states and localities, where these decisions should be made. Under the bill, states and localities can decide to support expansions or enforce more regulations on the short-term rental market and would not give online platforms a federal statute to avoid these laws.

This is a narrow, targeted change to the statute to ensure short-term rental companies and internet platforms comply with state and local planning, zoning, rental, labor and tax laws and end their abusive stretching of CDA 230's original intent. State attorneys general, mayors, and local officials have called for similar updates to CDA 230 to enable them to uphold their local laws and protect citizens living and working in their communities.

As your committee examines and updates CDA 230, I urge you to call for increased accountability for powerful internet platforms attempting to misuse CDA 230 to profit from illegal activity. The PLAN Act is one way to take such action, but I support broader efforts to

modernize the law to ensure that online platforms are not able to avoid legitimate local laws or profit from illegal activity in which they are complicit.

If you have any questions, please do not hesitate to let me or my office know.

Sincerely,

Ed Case
Ed Case
Member of Congress

Enclosure



October 10, 2019

Dear Members of Congress:

We are living in an economy where a few major tech companies are rapidly becoming so big and powerful that their business models are creating significant and harmful societal impacts. One of the most well-documented cases of this problem relates to the rising costs and decreasing availability of affordable housing.

The situation related to low- and moderate-income housing stock in many cities is a national crisis, and Big Tech short-term rental companies, like Airbnb and HomeAway, are adding to the problem. Across the country commercial investors are buying large swaths of residential homes for the sole purpose of converting them to permanent short-term rentals. This conversion is causing a reduction in the supply of housing, driving up the cost to rent or own a home and displacing families out of the neighborhoods they have called home for generations. Not surprisingly at all, mayors and city councils are working to craft solutions to this problem by regulating multi-unit real estate speculators who are using short term rental units as illegal hotels rather than rentals for low and middle income people.

However, when cities have been passing these kinds of reasonable regulations, lawyers for Airbnb and HomeAway are using Section 230 of the Communications Decency Act (CDA 230) to say they can't engage in any regulation of a tech company. This was never the intent of Section 230, which was written to foster free speech on the internet and allow companies with many users to post content without the company being sued.

Section 230 of the Communications Decency Act (CDA 230) shields websites from liability for content produced by third-party users on their platforms. Internet based short-term rental platforms invoke this protection when called to account for illegal rental activity they have facilitated even though they're intricately involved in every detail of the illegal listing. These companies collect and remit money, provide insurance, suggest pricing, hire photographers, making them a vital part of the transaction rather than a passive platform providing their users a space on the internet to share content. These companies are

knowingly facilitating and profiting from illegal listings all-the-while driving up the cost and access to housing and they must be held accountable.

Study after study shows Airbnb is depleting our housing stock across the country while driving up the cost to rent or own a home:

- The Economic Policy Institute [evaluated the costs and benefits of Airbnb-type rentals](#) and found that "the single biggest cost Airbnb imposes on communities is limiting the number of long-term rental housing units. Because housing demand is relatively "inelastic" (people's demand for somewhere to live doesn't decline when prices increase), even small changes in housing supply—like those caused

by converting long-term rental properties to Airbnb units—can cause significant price increases for local residents.”

- According to a [study](#) by the University Of California, Los Angeles (UCLA), Airbnb “Airbnb incentivizes landlords to remove properties from the long-term rental market...causing rents for long-term leases to increase.”
- McGill University conducted a [study](#) with a clear and undisputable conclusion that “the more Airbnbs in a city, the higher rents get for local residents” as Airbnb rentals have removed up to 13,500 housing units from the long-term market in New York City.

We urge you to support the Protecting Local Authority and Neighborhoods Act (PLAN Act) H.R. 4232 which will end the exploitation of CDA 230 by Big Tech platforms like Airbnb and HomeAway. Introduced by Congressman Ed Case, the PLAN Act will be a narrow clarification to the CDA 230 language, clarifying that CDA 230 does not shield short-term rental platforms from accountability when they facilitate illegal rental bookings.

This change will ensure short-term rental companies comply with state and local laws, put an end to their abusive exploitation of CDA 230’s original intent and help protect vital affordable housing across the country.

Sincerely,

American Family Voices (AFV)
 Blue Future
 Coalition for Economic Survival (CES)
 Community Change
 Courage Campaign
 Disability Power and Pride
 Hawaii Thousand Friends
 HI Good Neighbor
 International Center for Appropriate & Sustainable Technology
 Keep Neighborhoods First
 Kuli'ou'ou / Kalani Iki Neighborhood Board
 LAANE
 National Community Development Association
 New York Communities for Change
 People’s Action
 Save Oahu’s Neighborhoods (SONHawai‘i)
 Southeast Asian Community Alliance (SEACA)
 Strategic Actions for a Just Economy (SAJE)
 Venice Community Housing



i2Coalition Statement
"Fostering a Healthier Internet to Protect Consumers"
Joint Hearing of the House Energy and Commerce Subcommittees on
Communications and Technology and Consumer Protection and Commerce

October 16, 2019

The Internet contributes billions of dollars to the U.S. economy, touches nearly every aspect of the global economy, and helps promote human rights and democracy abroad.

Internet infrastructure providers are the companies supporting this tremendous vision, including web hosts, domain providers, cloud service providers, data centers, payment processors, software developers and more. These companies are providing a neutral, solid base upon which all the Internet's traffic and content flows.

The Internet Infrastructure Coalition (i2Coalition) represents nearly 100 leading businesses in this important industry and works to ensure that those who build the infrastructure of the Internet can continue to grow and innovate.

Intermediary protections contained in Section 230 of the Communications Decency Act are the key to Internet innovation. Section 230 establishes a framework where those responsible for content are held liable for their actions, rather than blaming infrastructure providers. The provision says: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" (47 U.S.C. § 230).

In other words, the kinds of Internet infrastructure companies the i2Coalition represents, that host, store, and replicate content, are intermediaries and not directly legally responsible as publishers for what others say and do on their services. Our companies simply enable people to create and consume content; they should not be held responsible for how people use these services. As an analogy, a telephone company isn't responsible for what people say to others using their services.

Policies attempting to make Internet intermediaries liable for all content flowing through their networks would impede i2Coalition members' ability to do business and place them in the position of policing content, a role better suited to law enforcement and the Courts.

The Internet is participatory, and users are allowed and encouraged to contribute content. It's common to look at that only in its most popular examples. Over 400



hours of video are uploaded to YouTube every minute. On Facebook, there are 317,000 status updates and 147,000 photos uploaded every 60 seconds.

While big social media platforms like Google, Twitter and Facebook enjoy the protections of Section 230, so do all the small businesses that have built the Internet. Congress must consider the impact of limiting intermediary protections on these small businesses (and the thousands of small business they serve) who need the protections of Section 230 to operate and survive. Given the amount of user-generated content on websites they support, it would be impossible to eradicate all objectionable or copyrighted content without stifling free speech. Holding companies responsible for their users' content would subject companies to lawsuits, and force limitations on how consumers use Internet platforms, at least within the United States of America. Voices would be censored because companies could not risk the legal liability of allowing content they deem risky to stay on their services.

Small companies would go out of business or more likely, relocate off-shore to innovate elsewhere, and the few large companies who could afford to stay would have strict content controls. Consumer choice would be decimated. We would revisit the era of old media, with fewer voices and more top-down control over what people say.

To understand the implications, imagine a world where your hosting provider, storage provider, or ISP needs to monitor your activity to make sure you aren't doing anything illegal. A hosting provider would likely comply with any third-party requests to take down content whether the request is legitimate or not.

Also, rather than providing encrypted, private cloud storage, providers could be barred from using encryption to allow for users' private content to be reviewed for potentially illegal material.

Without Section 230 protections, ISPs, since they connect users to online content, could block any websites or services that the ISP would deem questionable, which could apply to virtually every site featuring user-generated content. This could result in sweeping limitations of free speech and cut out many diverse voices.

Even Internet infrastructure providers who oversee the cables and servers that form the foundation of the Internet, who are not asking anyone to post or share information and who are neutral bodies, would now have to worry about content stored on their devices or that travels through their networks. They are not equipped to do this type of policing, nor should they.



Section 230 means that Internet companies can continue to perform their job of being a neutral conduit for their users, with legitimate courts making determinations about when content hosted on their network needs to be taken down.

Protecting an Internet infrastructure company's rights to host content as a neutral party was a smart move made back in the 90's that has allowed the Internet to grow and thrive.

The Internet has advanced free speech and the spread of information more so than any other invention our world has ever known, and it's too great of a responsibility for the mostly small businesses involved in delivering online content to judge the legality of their user's content. We urge Members of the Energy and Commerce Committee to recognize the importance of Section 230 and act to ensure its preservation.

Congress of the United States
Washington, DC 20515

May 3, 2019

Mr. Sundar Pichai
CEO, Google
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Pichai

Today we were made aware of Google Ads prohibiting promotions or advertisements that contain or show hunting practices. Google Ads' justification was that these promotions are considered 'animal cruelty' despite the fact that hunting is a core part of our natural heritage, a major component in environmental and wildlife conservation, and an integral part of our outdoor economy. We are not only deeply concerned with this prohibition, but believe that it is a troubling precedent for the exclusion of an important part of our national identity. Google should immediately change this policy interpretation to uphold our hunting and conservation heritage.

Montana's nickname as the Treasure State derives from the abundance of resources that exist throughout Montana's landscape. While Montana has a rich history in natural resources, nothing in the Treasure State is as deeply rooted in our heritage as hunting and a love of the great outdoors. As one of the most wild and pristine places in the lower 48, Montana's hunting tradition simply runs in our veins. As lifelong hunters, we have been blessed to spend time chasing wildlife in some of the most beautiful of places in the country with our grandparents, parents, spouses, and children. Sharing these experiences with our families and instilling an appreciation for wildlife and the outdoors in our children is one of the things we are most proud of, and we know Montanans of all different backgrounds would agree. Doing anything to minimize or jeopardize this great tradition is an affront to our values as Montanans and the respect we show to wildlife and the land we are so blessed to call home.

We therefore demand you reverse these prohibitions and request that Google reexamine their policy interpretations on prohibiting hunting promotions. We also request a meeting to discuss the importance of Montana's and the United States' hunting heritage.

Sincerely,


STEVE DAINES
United States Senator


GREG GIANFORTE
Member of Congress



October 15, 2019

Berin Szóka
President, TechFreedom
110 Maryland Ave, NE, #205
Washington D.C. 20002

Hon. Frank Pallone
Chairman
House Energy & Commerce Committee
House of Representative
2107 Rayburn House Office Building
Washington, DC 20515

Hon. Greg Walden
Ranking Member
House Energy & Commerce Committee
House of Representative
2185 Rayburn House Office Building
Washington, DC 20515

Re: Fostering Healthier Internet to Protect Consumers

Dear Chairman Pallone and Ranking Member Walden:

If one law has made today's Internet possible, it is Section 230 of the Communications Decency Act of 1996 ("Section 230").¹ Drafted by Rep. Chris Cox (R-CA) and Sen. Ron Wyden (D-OR), that law ensured that websites would not be held liable for content created by their users except in very limited circumstances. Without that law, social media sites that allow users to post content of their own creation would never have gotten off the ground, given the impossibility of monitoring user content at the scale at which such sites operate today. I write to correct several critical misconceptions that have plagued this debate.

I. There Was No "Quid Pro Quo" behind Section 230

The Republican Staff Memo claims that Section 230 reflects an implicit *quid pro quo*:

Congress included Section 230 to balance the need for creating a safe harbor for small Internet companies to innovate and flourish without fear of insurmountable legal fees, while also keeping the Internet clear of offensive and violent content by

¹ 47 U.S.C. § 230.

empowering Internet platforms to take action to clean up their own site. This has often been referred to as the “shield and sword,” where platforms receive a “shield” from liability for using the ability to self-regulate, or the “sword” that CDA 230 provides them.²

The memo then claims that “platforms” have failed to meet their end of the bargain: “Internet platforms have, in many instances, benefitted from the ‘shield’ without using the ‘sword’ as intended.”³ Both claims are false: the first misrepresents the legislative history of Section 230 and the second fails to acknowledge how much interactive computer service providers, both large and small, wield the “sword” of content moderation — and *why* they do so, without a legal mandate to.

A. Congress Intended Section 230 to Protect Operators from Having to Do the Impossible.

Nothing in the text of Section 230 suggests Congress intended to create “shield” for hosting or removing content in exchange for companies using a “sword” in removing content. Instead, the floor discussions of the bill make clear the Congress was focused on two things (1) protecting websites from having to do the impossible — and thus ensuring that the Internet would not be strangled in its crib the thread of legal liability and (2) removing legal disincentives that discouraged websites from using their “sword.” Consider the remarks of Rep. Bob Goodlatte (R-VA):

Mr. Chairman, I thank the gentleman from Oregon [Mr. WYDEN] for yielding this time to me, and I rise in strong support of the Cox-Wyden amendment. This will help to solve a very serious problem as we enter into the Internet age. We have the opportunity for every household in America, every family in America, soon to be able to have access to places like the Library of Congress, to have access to other major libraries of the world, universities, major publishers of information, news sources. *There is no way that any of those entities, like Prodigy, can take the responsibility to edit out information that is going to be coming in to them from all manner of sources onto their bulletin board. We are talking about something that is far larger than our daily newspaper. We are talking about something that is going to be thousands of pages of information every day, and to have that imposition imposed on them is wrong.* This will cure that problem, and I urge the Members to support the amendment.⁴

² Memorandum from the Republican Staff Committee to the Republican Members of the Committee on Energy and Commerce at 2 (Oct. 11, 2019). [hereinafter Republican Staff Committee Memo].

³ *Id.* at 4.

⁴ Congressional Record, *House Debate on Section 230* at H8471 (Aug. 4, 1995) (emphasis added).

Rep. Chris Cox, who drafted the law personally, made clear that he aimed to remove the perverse disincentives created by the legal system. His discussion of the then-recent court decisions that drove him to draft Section 230 is worth reprinting in its entirety:

Mr. Chairman, what we want are results. We want to make sure we do something that actually works. Ironically, *the existing legal system provides a massive disincentive for the people who might best help us control the Internet to do so.*

I will give you two quick examples: A Federal court in New York, in a case involving CompuServe, one of our online service providers, held that CompuServe would not be liable in a defamation case because it was not the publisher or editor of the material. It just let everything come onto your computer without, in any way, trying to screen it or control it. But another New York court, the New York Supreme Court, held that Prodigy, CompuServe's competitor, could be held liable in a \$200 million defamation case because someone had posted on one of their bulletin boards, a financial bulletin board, some remarks that apparently were untrue about an investment bank, that the investment bank would go out of business and was run by crooks. Prodigy said, "No, no; just like CompuServe, we did not control or edit that information, nor could we, frankly. We have over 60,000 of these messages each day, we have over 2 million subscribers, and so you cannot proceed with this kind of a case against us." The court said, "No, no, no, no, you are different; you are different than CompuServe because you are a family-friendly network. You advertise yourself as such. You employ screening and blocking software that keeps obscenity off of your network. You have people who are hired to exercise an emergency delete function to keep that kind of material away from your subscribers. You don't permit nudity on your system. You have content guidelines. You, therefore, are going to face higher, stricter liability because you tried to exercise some control over offensive material.

Mr. Chairman, that is backward. We want to encourage people like Prodigy, like CompuServe, like America Online, like the new Microsoft network, to do everything possible for us, the customer, to help us control, at the portals of our computer, at the front door of our house, what comes in and what our children see. This technology is very quickly becoming available, and in fact every one of us will be able to tailor what we see to our own tastes.

We can go much further, Mr. Chairman, than blocking obscenity or indecency, whatever that means in its loose interpretations. We can keep away from our children things not only prohibited by law, but prohibited by parents. That is where we should be headed, and that is what the gentleman from Oregon [Mr. WYDEN] and I are doing.

Mr. Chairman, our amendment will do two basic things: First, it will *protect computer Good Samaritans, online service providers, anyone who provides a front end to the Internet, let us say, who takes steps to screen indecency and offensive material for their customers. It will protect them from taking on liability such as occurred in the Prodigy case in New York that they should not face for helping us and for helping us solve this problem.* Second, it will establish as the policy of the United States that we do not wish to have content regulation by the Federal Government of what is on the Internet, that we do not wish to have a Federal Computer Commission with an army of bureaucrats regulating the Internet because frankly the Internet has grown up to be what it is without that kind of help from the Government. In this fashion we can encourage what is right now the most energetic technological revolution that any of us has ever witnessed. We can make it better. We can make sure that it operates more quickly to solve our problem of keeping pornography away from our kids, keeping offensive material away from our kids, and I am very excited about it.⁵

So while the Republican Staff memo links the “sword” and “shield” as part of a quid pro quo, the legislative history of Section 230 makes clear that the law intended to protect *both* those that did no content moderation (then protected under the legal rule announced in *Cubby, Inc. v. CompuServe, Inc.*⁶), as well as those that *did* engage in content removal (left exposed under the theory espoused in *Stratton Oakmont v. Prodigy Services Co.*⁷). Congress never intended a link, or a *quid pro quo*, between content moderation and immunization from liability for third-party content.

B. Website Operators Do Engage In Active Content Moderation

Internet services rely heavily on the sword just as much as the shield to manage their reputation and maintain their competitive edge in the market. The memo appears to suggest that the shift towards an “advertising-centric business models built upon user-generated content” has made websites less willing to wield the sword of content moderation.⁸ In fact, just the opposite is true: relying on advertising generally gives platforms *more* of an incentive to monitor and remove objectionable user content.

There are, of course, exceptions — but they prove our point. Backpage derived the bulk of its revenues from sex trafficking ads. As discussed below, we have always believed the company

⁵ Cong. Rec. at H8470 (1995) (statement of Rep. Chris Cox).

⁶ *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).

⁷ *Stratton Oakmont v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. 1995).

⁸ Republican Staff Committee Memo, *supra* note 2, at 3-4.

could have, and should have, been prosecuted even without new federal legislation because (a) Section 230 does not shield any site from criminal liability and (b) the company lost the protections of Section 230 by helping to create sex trafficking ads. More generally, we believe the primary response to sites like Backpage should be the enforcement of existing criminal laws and, if necessary, the creation of new laws carefully targeted to address that conduct *without* burdening lawful speech. That can be done *without* amending Section 230.

II. The Republican Staff Memo Misunderstands Three Other Key Aspects of Section 230

The Republican Staff Memo claims that Section 230 has been interpreted more broadly than Congress intended: “While the authors intended this liability protection to incentivize ‘interactive computer services’ to patrol their platforms, it was not intended to be interpreted as an unlimited, broad liability protection absent any good faith action to maintain accountability.”⁹ This sentence is misleading in three respects — both essential to properly understanding Section 230. The Republican memo overstates the scope of Section 230’s immunity by failing to mention two kinds of limitations upon that immunity: explicit carve-outs and liability for content that operators help to create. Finally, the memo makes the unsupported claim that Congress expected more “good faith action to maintain accountability” as a condition of Section 230’s protections.

A. Section 230 Explicitly Preserves Four Sources of Liability

As the Democratic Staff Memo notes, “CDA 230 does provide some exceptions to this immunity. Websites may still be held liable for third-party content that violates: (1) federal criminal law; (2) intellectual property law; (3) the Electronic Communications Privacy Act; and (4) certain laws prohibiting sex trafficking.” The Republican Staff memo mentions only the last of these — a recent amendment — failing to mention that the first three exceptions are written directly into the statute.¹⁰ These exceptions, particularly those for federal criminal and intellectual property claims, are major and longstanding sources of potential liability for online service operators.

⁹ Republican Staff Committee Memo, *supra* note 2, at 2.

¹⁰ The Republican Memo does mention that “Section 230(c)(2) of the Communications Act provides a *civil* liability safe harbor for ‘interactive computer services’ that voluntarily, in good faith, take actions to restrict access to obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable content,” Republican Staff Committee Memo, *supra* note 2, at 1 (emphasis added). This oblique reference is simply inadequate to convey the inverse: that Section 230 has never immunized websites from *criminal* liability.

That Section 230 does not affect liability for intellectual property violations — and, in particular, copyright violations, which are covered by the Digital Millennium Copyright Act¹¹ — is a source of perpetual confusion in coverage of these debates. This point merits special emphasis because much of the attack on Section 230 seems to be coming from copyright interests who, presumably, know better but seem to benefit politically from confusing Section 230 with liability for copyright violations.

But the most important explicit limitation of the Section’s protections is that for liability under federal criminal law. On the one hand, there are already a host of federal laws under which service operators can be charged, including broad liability for conspiracy and racketeering, with ample monetary remedies available upon conviction, including asset forfeiture. On the other hand, this exception means that Congress has always had the ability to combat online ills by creating new federal criminal laws — *without* the need to amend Section 230. The House version of the Allow States and Victims to Fight Online Sex-Trafficking Act (FOSTA) would have done precisely this;¹² we supported that piece of legislation as a targeted solution for the scourge of online sex trafficking, but opposed combining that bill with the Senate’s Stop Enabling Sex Trafficking Act (SESTA), which created broad new *civil* liability as a new exception to Section 230.¹³

B. Section 230 Does not Protect Service Operators from Liability for Content They Help to Create.

Importantly, as the Democratic Staff Memo also notes, “CDA 230 does not protect a website from liability for its own content.”¹⁴ The Republican Staff Memo mentions that Section 230 “provides a liability shield to ‘interactive computer services’ from being treated as a publisher or speaker of any information provided by another information content provider.”¹⁵ The Democratic Staff Memo says essentially the same thing.¹⁶ Both paraphrase the wording

¹¹ 17 U.S.C. § 512.

¹² H.R. Rep. No. 115-572 on H.R. 8165 Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (Feb. 20, 2018), available at <https://www.congress.gov/congressional-report/115th-congress/house-report/572>

¹³ Letter from TechFreedom joined by policy organizations to lawmakers (Feb. 23, 2018), available at http://docs.techfreedom.org/Letter_SESTA-FOSTA_Hybrid_2-23-18.pdf

¹⁴ Memorandum from Committee on Energy and Commerce Staff to Subcommittee on Communications and Technology and Subcommittee on Consumer Protection and Commerce Members and Staff at 3 (Oct. 11, 2019). [hereinafter Democratic Staff Committee Memo].

¹⁵ Republican Staff Committee Memo, *supra* note 2, at 1 citing 47 U.S.C. §230.

¹⁶ The Democratic Memo mentions “First, CDA 230 prohibits courts from treating “an interactive computer service”—a web-based platform— “as the publisher or speaker” of material posted on the site by third-parties,” Democratic Staff Committee Memo, *supra* note 14, at 3.

of Section 230(c)(1) and, in so doing, omit what former Rep. Christopher Cox (R-CA) has called the “two most important words” in Section 230.¹⁷ Information *content* providers (ICPs) are *not* shielded from immunity by the statute. An ICP is defined as “any person or entity that is responsible, in whole or *in part*, for the creation or development of information provided through the Internet or any other interactive computer service.”¹⁸ The importance of the words “in part” is easy to miss because these words are found not in the functional provisions of the statute but in the definition of an information content provider.

These two words have allowed the courts to delineate when websites cross the line from merely hosting (or otherwise making available) user content to actually helping to create or develop it. For example:

- Roommates.com was held to have lost the protection of Section 230 and be liable under federal fair housing laws for helping to create racially discriminatory ads because the site solicited racial preferences of its users.¹⁹
- Backpage.com hired a company based in the Philippines to scour other websites for ads that could run on Backpage, create accounts on Backpage for those users, copy their ads onto Backpage, contact those users, and encourage them to switch to Backpage — as revealed in a June 2017 expose in *The Washington Post*.²⁰ On April 6, 2018 before FOSTA was signed into law, the DOJ and state AGs shut down Backpage and obtained a guilty plea from its CEO using *existing* federal criminal law.²¹
- Accusearch created a service that collected confidential phone numbers, weaponizing private data for commercial gain. Because Accusearch “developed” the offending content, they were responsible at least *in part* and thus could be sued by the Federal Trade Commission.²²

¹⁷ Armchair discussion with Former Congressman Cox, Back to the Future of Tech Policy, YouTube (August 10, 2017), available at https://www.youtube.com/watch?time_continue=248&v=iBEWXIn0IUy

¹⁸ 47 U.S.C. § 230(f)(3) (emphasis added).

¹⁹ *Fair Hous. Council v. Roommates.com, LLC*, 521 F.3d 1157, 1174 (9th Cir. 2008).

²⁰ Tom Jackman and Jonathan O’Connell, *Backpage has always claimed it doesn’t control sex-related ads. New documents show otherwise* (2017), available at https://www.washingtonpost.com/local/public-safety/backpage-has-always-claimed-it-doesnt-control-sex-related-ads-new-documents-show-otherwise/2017/07/10/b3158ef6-553c-11e7-b38e-35fd8e0c288f_story.html

²¹ Christine Biederman, *Inside Backpage.com’s Vicious Battle with the Feds* (2019), available at <https://www.wired.com/story/inside-backpage-vicious-battle-feds/>

²² *FTC v. Accusearch*, 570 F.3d 1189 (2009). For more information see Michael Erdman, *Website (search engine?) not entitled to Section 230 protection for FTC Act violation* (2007), available at <https://onlineliabilityblog.com/2007/10/27/website-search-engine-not-entitled-to-section-230-protection-for-ftc-act-violation/>

C. Congress Wisely Required “Good Faith” for Content Removal, but not Publishing.

Again, the Republican Staff Memo claims that Section 230 “was not intended to be interpreted as an unlimited, broad liability protection absent any good faith action to maintain accountability.” As demonstrated above, Section 230’s immunity is neither “unlimited” nor as “broad” as the Republican Staff Memo claims.

That memo’s claim about “good faith” is also misleading. In fact, Congress’s intention is unmistakable from the plain text of the statute. Section 230(c)(2)(A)’s immunity for removal of content (to paraphrase that subsection) explicitly requires good faith while Section 230(c)(1)’s immunity for publishing content does not. As discussed below, Congress clearly knew what it was doing in writing a good faith requirement into one provision but not the other. One could hardly find a clearer case of the statutory canon of *expressio unius est exclusio alterius*: “the express mention of one thing of a type may excludes others of that type.”²³

D. Section 230(c)(2)(A)’s Good Faith Requirement Has Properly Been Interpreted Narrowly.

Because most cases are resolved on 230(c)(1) grounds, there is relatively little case law on the meaning of “good faith.” In 2011, Santa Clara Law Prof. Eric Goldman, having done an exhaustive survey of Section 230 case law, concluded that “no online provider has lost § 230(c)(2) immunity because it did not make a good faith filtering decision.”²⁴ “Nevertheless, even the relatively few judicial decisions have provided examples of some provider actions that may not be in good faith. For example, anticompetitive motivations might disqualify an online provider from § 230(c)(2).”²⁵ In another case, “the judge found that an online provider’s failure to articulate a reason for its blocking decision could be bad faith.”²⁶ Prof. Goldman concluded:

As these examples illustrate, the statute’s “good faith” reference invites judges to introduce their own normative values into the consideration. Fortunately, most judges do not introduce their own normative values into the statutory inquiry.

²³ *Encino Motorcars, LLC v. Navarro*, 136 S. Ct. 2117 (2016).

²⁴ Eric Goldman, *Online User Account Termination and 47 U.S.C. §230(c)(2)*, 2 UC Irvine Law Rev. 659, 665 (2012), available at <https://ssrn.com/abstract=1934310>

²⁵ *Id.*

²⁶ *Id.* citing *Smith v. Trusted Universal Standards in Elec. Transactions*, No. 09-4567 (RBK/KMW), 2011 WL 900096, at *25–26 (D.N.J. Mar. 15, 2011).

Several § 230(c)(2) cases have held that good faith is determined subjectively, not objectively.²⁷

Some may see this narrow application as a defect in the law, but it probably reflects the underlying constitutional issue: The First Amendment protects private actors in their exercise of editorial discretion, which is precisely what both Section 230(c)(2)(A) and 230(c)(1) protect.²⁸ The First Amendment does not, of course, protect anti-competitive conduct, even by media companies, and thus is it not surprising that anti-competitive conduct should be considered not in good faith.²⁹ Likewise, the First Amendment may allow for some degree of mandatory transparency as to *how* editorial discretion is exercised.

Congress should tread very, very carefully here, as we have previously urged the House Judiciary Committee in testimony, lest it create a system of legal mandates even more intrusive than the Fairness doctrine was. Any attempt to extend regulations from the broadcasting world would be obviously unconstitutional, since those regulations depend on the specific limitations the Supreme Court has placed upon the First Amendment rights of broadcasters.³⁰ Those limitations may not stand up to First Amendment review if challenged today, but even if they are still valid, they are specific to broadcasting, and do *not* apply to Internet media, which the Court has made clear enjoy the full protection of the First Amendment.³¹

If lawmakers want to better understand how Section 230 has been applied, a more detailed study of the case law on the “good faith” standard would be an excellent place to start.

III. Congress Struck the Right Balance in Crafting Section 230

Congress had good reasons for not making Section 230(c)(1) contingent upon “good faith;” doing so would have completely changed the dynamics of how Section 230 works, largely defeating the purpose of Section 230: protecting service operators from having to litigate every lawsuit brought against them. There is a world of difference between being able to dismiss a lawsuit with a standard motion to dismiss on a pure question of law (arguing that

²⁷ *Id.* citing (on the subjectivity of good faith) *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169 (9th Cir. 2009); *e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605 (N.D. Ill. 2008). *But see* Nat’l Numismatic Certification, LLC v. eBay, Inc., No. 6:08-cv-42-Orl-19GJK, 2008 WL 2704404 (M.D. Fla. July 8, 2008).

²⁸ Berin Szóka, *Platform Responsibility & Section 230 Filtering Practices of Social Media Platforms: Hearing Before the House Committee on the Judiciary*, (April 2018), available at http://docs.techfreedom.org/Szoka_Testimony-Platform_Responsibility_&_Neutrality-4-25-18.pdf

²⁹ Letter from TechFreedom joined by policy organizations and experts to Jeff Sessions (Sept. 21, 2018), available at <https://techfreedom.org/wp-content/uploads/2018/09/Letter-to-Jeff-Sessions-re-Social-Media-Bias-v2.pdf>

³⁰ *Id.*

³¹ *Reno v. ACLU*, 521 U.S. 844 (1997) (striking down federal law governing online child protection).

the plaintiff had failed to show that the site had lost its Section 230 immunity, principally by becoming responsible, at least in part, for developing content) and having to endure discovery by the plaintiff, having to draft a motion for summary judgment specific to the facts of the case, and having to litigate that motion. Multiply the increased cost and hassle of the latter by the enormous number of lawsuits a website might face if Section 230(c)(1) included a good faith requirement, given the staggering scale of Internet services, and Section 230 would be a fundamentally different statute. Under such a statute, nothing like the Internet as we know it could have developed. Digital services would look much more like Netflix, Spotify, or cable, focused on content created by digital publishers, rather than users.

Judge Alex Kozinski summarized the problem best in his *Roommates.com* decision. Even as he ruled that the website was, in fact, responsible, at least “in part,” for creating racially discriminatory housing ads, he cautioned that plaintiffs (and state prosecutors) must bear the burden of establishing that a website had lost the protection of Section 230:

We must keep firmly in mind that this is an immunity statute we are expounding, a provision enacted to protect websites against the evil of liability for failure to remove offensive content. Websites are complicated enterprises, and there will always be close cases where a clever lawyer could argue that something the website operator did encouraged the illegality. Such *close cases, we believe, must be resolved in favor of immunity, lest we cut the heart out of section 230 by forcing websites to face death by ten thousand duck-bites, fighting off claims that they promoted or encouraged — or at least tacitly assented to — the illegality of third parties.*³²

Any proposed amendment to Section 230 should be assessed on this basis: will it force websites to “face death by ten thousand duck-bites?”

One proposal that clearly fails that test is the amendment to Section 230(c)(1) proposed by Prof. Danielle Citron, one of the witnesses at this hearing, and Ben Wittes:

No provider or user of an interactive computer service that *takes reasonable steps to prevent or address unlawful uses of its services* shall be treated as the publisher or speaker of any information provided by another information content provider in any action arising out of the publication of content provided by that information content provider.³³

³² *Fair Hous. Council v. Roommates.com, LLC*, 521 F.3d 1157, 1174 (9th Cir. 2008) (emphasis added).

³³ Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 *FORDHAM L. REV.* 401, 419 (2017).

While this proposal may sound moderate, it would make Section 230's principal protection dependent upon a triable question of fact. Plaintiffs would be able to insist upon extensive discovery into how operators run their services to assess the reasonableness of their practices. What is "reasonable" is literally the most litigated question in the English language.³⁴

IV. Congress Wisely Did Not Include a Size Threshold in Section 230

The Republican Staff Memo includes another unsubstantiated claim about legislative intent: "Congress included Section 230 to balance the need for creating a safe harbor for *small* Internet companies to innovate and flourish without fear of insurmountable legal fees."³⁵ The memo goes on to identify size as one of the "issues" that "Congress has been reviewing" in determining "what constitutes an 'interactive computer service.'"³⁶ The memo reads as follows:

1. The Size of the Platform is Relevant.

The size, scale, sophistication, and influence of Internet platforms during the time CDA 230 was written is drastically different than today's Internet. While the liability protection for small, nascent Internet platforms in 1996 may have created the Internet we know today, the reality is that many Internet platforms today are much larger, some having market valuations nearing \$1 trillion dollars. With such available resources, Internet platforms have come under greater scrutiny to use their "sword" and create accountability on their platform.³⁷

The White House is reportedly drafting an Executive Order that would ask the Federal Communications Commission to issue a declaratory ruling that would narrow the definition of "interactive computer service" to exclude leading social networks.

These proposals fundamentally misunderstand what Section 230 was intended to do. The law was not simply a shield for nascent industry. In 1996, AOL already had 5 million users,

³⁴ "...such amorphous eligibility standards would negate or completely eliminate Section 230's procedural benefits. It would make Section 230 litigation far less predictable, and it would require expensive and lengthy factual inquiries into all evidence probative of the reasonableness of defendant's behavior," Eric Goldman, *Why Section 230 Than the First Amendment*, Notre Dame Law Review Online, Forthcoming (March 12, 2019), available at <https://ssrn.com/abstract=3351323>

³⁵ Republican Staff Committee Memo, *supra* note 2, at 2.

³⁶ *Id.*

³⁷ *Id.*

and was adding subscribers rapidly.³⁸ Congress certainly could not have imagined what today's Internet would look like, but certainly did understand that the "small, nascent Internet platforms" were growing explosively. Congress could have built size thresholds into the statute but did not do so — because size was essentially irrelevant.

What mattered to Congress then, and what matters now, is not how deep a company's pockets are, but what the effect of making them liable for user content will be *on the margins*. Even the best-resourced company in the world may decide that facing "death by ten thousand duck bites" simply is not worth it. Even the world's largest social media platforms cannot possibly replicate the kind of fact-checking that traditional media do for the third party content they host (like letters to the editor and obituaries). In any event, what matters is not "whether a company can afford it" but what the effect of increased liability would be *on users themselves*. Section 230 was intended both to enable websites to host user speech (Section 230(c)(1)) and also to remove objectionable content ((Section 230(c)(2)(A)). The law was carefully crafted to achieve both goals simultaneously. Congress should be exceedingly careful about disrupting that balance.

V. How Section 230 Applies to Other Digital Intermediaries

The Republican Staff Memo correctly notes that the world has become ever more complicated since Section 230 was enacted:

In addition to the increasing size and sophistication of Internet platforms, the Internet's architecture has become more complex since CDA 230 was enacted. Whereas the 1996 law envisioned a simple world of "interactive computer services," today's Internet requires a more complex web of edge providers, content delivery networks (CDNs), ISPs, and others that have a distinct role in creating today's Internet experience. In some instances, CDNs have played a very explicit and public role in moderating speech.

But this is hardly an argument for amending Section 230. And it is in this arena that Congress could do the most damage in amending Section 230, given the complexity of this space. As we noted in a statement of principles we helped to draft in July, signed by 53 leading experts in intermediary liability and Internet law, and 27 other organizations:

Principle #7: Section 230 should apply equally across a broad spectrum of online services. Section 230 applies to services that users never interact with directly. The further removed an Internet service—such as a DDOS protection provider or

³⁸ CNBC, *Timeline: AOL through the Years* (2015), available at <https://www.cnbc.com/2015/05/12/timeline-aol-through-the-years.html>

domain name registrar—is from an offending user’s content or actions, the more blunt its tools to combat objectionable content become. Unlike social media companies or other user-facing services, infrastructure providers cannot take measures like removing individual posts or comments. Instead, they can only shutter entire sites or services, thus risking significant collateral damage to inoffensive or harmless content. Requirements drafted with user-facing services in mind will likely not work for these non-user-facing services.³⁹

It is in this area that Congress risks doing the most fundamental damage to the Internet itself.

VI. The False Argument for Regulatory Asymmetry

The Republican Staff Memo identifies, as one of the “issues” to be discussed, “Regulatory Asymmetry”:

Internet platforms make editorial judgements regarding: what content is and is not permissible, what content users do and do not see, and whether certain users are or are not allowed to exercise online speech, which can be viewed inconsistent with their status as third-party intermediaries. By contrast, *traditional media companies are held accountable for the news content they publish online*. This inconsistent treatment of Internet platforms and traditional media companies may impact both industry competition and consumer protection.

This completely misstates the law and reveals a profound misunderstanding of how Section 230 works. In fact, traditional media companies enjoy precisely the same protections of Section 230 for their online operations as “new media” because Section 230 applies equally to *all* “interactive computer service providers.” That is, neither kind of company can be held civilly liable for content created by third parties unless it can be shown that they shared in creating it. Thus, for example, the user comments on a *New York Times* story posted on the Internet are treated exactly like the comments posted on Facebook or a community knitting discussion board. Likewise, Fox News is responsible for the content it creates and posts to the Internet, just as Facebook is responsible for its own posts. What matters is not the identity of the company, but who is responsible for developing the content.

There is no regulatory or legal “asymmetry” about a newspaper being held responsible for “publishing” its own content online simply because creating its own content is the bulk of what the site does, while Facebook primarily hosts content created by users. This simply

³⁹ *Liability for User-Generated Content Online Principles for Lawmakers* (2019), available at <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2992&context=historical>

reflects the fact that these media companies work very differently. There is no reason to expect that such different companies should be subject to the same legal regimes. The crucial difference lies in the problem of scale: traditional media companies can screen the third party content they host, such as letters to the editor, advertisements, classifieds, obituaries, and the like. Internet services cannot, because they handle exponentially greater volumes of content. It is no response to say, as some conservatives now do, that such companies simply should not exist — but it is at least an honest recognition of the reality highlighted back in 1996 by Rep. Goodlatte: content moderation at scale is so inherently difficult that exposing companies to civil liability for the decisions they make will either (a) simply eliminate such services or (b) have the perverse effect of disincentivizing them from *trying* to remove harmful or objectionable content.

VII. The Underlying Constitutional Constraints Facing Congress

Websites are private media companies that enjoy the full protection of the First Amendment — unlike broadcasters, whose First Amendment rights have been limited because they use the public airwaves.⁴⁰

It is true that “Internet platforms have come under greater scrutiny to use their ‘sword’ and create accountability on their platform,”⁴¹ but that is a question of politics, not of what the law — or even what it *should* be. In assessing what the law should be, lawmakers must realize that what we are talking about is essentially regulation of speech. There is very little (if anything) the government can lawfully do to directly require website operators to clean up lawful speech. The Supreme Court made that clear in striking down every other provision of the Communications Decency Act of 1996 *besides* Section 230,⁴² as did the lower courts in striking down the Child Online Protection Act of 1998.⁴³ Fundamentally, Section 230 can best be understood as a way to ensure that private actors will not be deterred by fear of civil liability from attempting to police online content *as they see fit* — thus protecting their editorial discretion and avoiding a First Amendment challenge.

⁴⁰ Szóka Testimony at 13.

⁴¹ Republican Staff Committee Memo, *supra* note 2, at 5.

⁴² *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

⁴³ Child Online Protection Act, Pub. L. No. 105-277, 112 Stat. 2681-736, § 1403 (codified at 47 U.S.C. § 231), enjoined from enforcement in alternative part by *American Civil Liberties Union v. Mukasey*, 534 F.3d 181 (3d Cir. 2008) (prohibiting enforcement of COPA’s civil and criminal penalties contained in 47 U.S.C. § 231(a)(1)), cert. denied 555 U.S. 1137.

Any attempt to rework Section 230 to force digital media companies to police or host content in ways they would not otherwise have done faces the same sort of First Amendment problems, even if they are one step removed. We discussed these issues in our House Judiciary Committee testimony.⁴⁴ Professor Larry Tribe summarized the case law thusly: “government may not condition the receipt of its benefits upon the nonassertion of constitutional rights even if receipt of such benefits is in all other respects a ‘mere privilege.’”⁴⁵

VIII. Conclusion

Congress made a complete mess of SESTA, the first amendment to Section 230 since the law was enacted in 1996. The list of procedural fouls is long, but among others, the Senate bill (amending Section 230) never went through the Senate Judiciary Committee, the bill was married to a completely different House bill (that did not amend Section 230) on the House floor, and at the end of the day, the specific website it was targeting was prosecuted under existing law anyway. Congress never developed a clear grasp of the issues at stake, leaving fundamental questions unanswered, including what prosecutions and civil actions were actually possible under Section 230 and existing law. Congress must not make the same mistakes again. If lawmakers feel they must act, the best next step would be to order a study of these issues by a blue ribbon commission of experts.

Republicans, in particular, should remember that Section 230 was drafted by a Republican Congressman (who went on to serve a long and distinguished career as a Republican), supported by leading Republicans, and enacted with overwhelming Republican support. It is also the most successful Republican tort reform measure in history, ensuring that the threat of litigation did not stifle a potentially thriving industry. Section 230 is one of the greatest bipartisan success stories of all time. Any discussion of amending Section 230 should be addressed in the same thorough and bipartisan manner.

Sincerely,

_____/s/_____
 Berin Szóka
 President, TechFreedom
bszoka@techfreedom.org

⁴⁴ Szóka Testimony at 22.

⁴⁵ L. TRIBE, AMERICAN CONSTITUTIONAL LAW 510 (1st. ed. 1978).



October 16, 2019

Chairman Frank Pallone
Ranking Member Greg Walden
House Committee on Energy & Commerce
Rayburn House Office Building 2125
Washington, D.C. 20515

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

Internet Association¹ (IA) welcomes the opportunity to submit this letter for the record as part of the Committee's October 16th hearing: *"Fostering a Healthier Internet to Protect Consumers."* IA is the only trade association that exclusively represents leading global internet companies on matters of public policy. Our mission is to foster innovation, promote economic growth, and empower people through the free and open internet. We believe the internet creates unprecedented benefits for society, and as the voice of the world's leading internet companies, Internet Association works to ensure legislators, consumers, and other stakeholders understand these benefits.

The internet is integral to our way of life, but if we don't maintain sound public policy protecting its use, we could lose the services that we most value.

Passed as part of the Communications Decency Act in 1996, CDA 230 created two key legal principles. First, online platforms are not the speaker of user-generated content posted on their websites – all the social media posts, memes, photos, professional information, dating profiles, product reviews, and ratings people post online. And second, that these online platforms – whether they're schools, libraries, neighbors who run list-serves in our communities, volunteers who run soccer leagues, bloggers, citizen journalists, churches, labor unions, or anyone else that may offer a space for online communications – can moderate and delete harmful or illegal content posted on their platform. Most online platforms – and all of IA's members – have robust codes of conduct, and CDA 230 allows the platforms to enforce them.

In practice, CDA 230 enables what many would consider the best of the internet. It allows internet users to post their own content and engage with the content of others, whether that's friends, family, co-workers, companies posting jobs, someone posting an apartment for rent, fellow gamers, or complete strangers from the other side of the globe with a shared experience.

¹ Internet Association represents <https://internetassociation.org/our-members/>.



Returning to the world before 230 was passed would mean platforms who do not make any attempt to moderate content would escape liability, but those who moderate would have the same liability as if they themselves wrote the content. On the one hand, you would have platforms with highly volatile, unregulated, and potentially dangerous content that is posted without review. Internet companies in this camp would be incentivized to have no knowledge of anything on their platform. And on the other hand, you would have platforms that host only highly-curated, editorial-like content with significantly fewer voices. The flourishing middle ground we enjoy today would cease to exist.

We've come to take for granted the millions of good things that happen every day because of the internet. Stopping bad actors online can be accomplished without removing a fundamental pillar on which the modern internet was built. The actions that policy makers want online platforms to take against a wide range of inappropriate content are enabled by Section 230 and platforms acting responsibly should be encouraged.

The nation's leading internet companies agree they should voluntarily undertake content moderation activity to promote online and real world safety and they do – whether using hash values to identify child sexual abuse imagery, using algorithms to detect ISIS and other terrorist content, providing resources to users threatening suicide, or taking thousands of other actions daily to remove harmful content. CDA 230 is the law that allows that to happen. Let's ensure we are approaching this issue with the big picture in mind.

Thank you again for the opportunity to submit this letter for the record and we look forward to being a resource to the Committee going forward.

Sincerely,

A handwritten signature in black ink, appearing to read 'Michael Beckerman'.

Michael Beckerman
President and CEO



October 15, 2019

Re: Fostering a Healthier Internet to Protect Consumers

Dear Chairman Pallone, Ranking Member Walden, Chairman Doyle, Ranking Member Latta, Chairwoman Schakowsky, Ranking Member McMorris, and Members of the Committee:

The Wikimedia Foundation appreciates the opportunity to submit comments for the record on the hearing entitled “Fostering a Healthier Internet to Protect Consumers.” As the non-profit organization that hosts and supports Wikipedia, among other projects, the Foundation relies upon the protections of Section 230 in order to exist and operate. Wikipedia could not exist were it not for Section 230. Therefore, proposed changes to the law should be carefully considered to ensure that they do not drastically increase liability for online platforms like Wikipedia, or disincentivize good-faith moderation by staff or volunteers.

Wikipedia has become one of the most visited websites in the world through the efforts of tens of thousands of volunteers who contribute articles, edit them, and reconcile differences between each others’ edits. The contents of Wikipedia are therefore truly user-generated, covering a vast number of topics far outside the knowledge, let alone expertise, of any Foundation staff. These edits occur at a rate of 1.8 every second, and while most of them are adding to or refining the knowledge freely available on the site, some will consist of pranks, propaganda, or mistakes, many of which could amount to defamation or create other liabilities that can attach to speech.

The Need for Section 230 and the Necessary Interaction between 230(c)(1) and (c)(2)

Section 230(c)(1) is the reason that Wikipedia can operate with certainty that it will not face extraordinary liability exposure, and it is therefore essential to our mission of ensuring that the world’s knowledge can be shared freely. Section 230(c)(2) also ensures that, despite a strong ethic of sharing all types of information, Wikipedia’s content can be moderated by its users and administrators.

The community-developed rules for what is permitted in Wikipedia articles may differ in many ways from the types of rules on more conversation-oriented platforms. For example, content policies prohibit editors from including their original research in articles, even if that material is accurate and neutral. Without this rule, Wikipedia would be less of an encyclopedia and more like a

Imagine a world in which every single human being can freely share in the sum of all knowledge.



forum for users to post the results of their research, with potentially detrimental effects on its reliability and verifiability.

This idiosyncratic rule—one that might appear arbitrary in the abstract—actually shapes Wikipedia as a platform. This is one example of what communication scholar Tarleton Gillespie means when he says that moderation makes platforms: that content moderation is not just a function of a platform, but that it defines what the platform is.¹

The importance of this is not limited to the idea that section 230(c)(2) should continue to permit flexibility in platforms’ content moderation. There is a tendency to separate the two parts of 230(c) and to treat them separately as though each has a completely separate purpose: (c)(1) to provide a limitation on liability, and (c)(2) to encourage content moderation. Regardless of what legislative historians and legal scholars might conclude about this, the practical reality for most online platforms is that the two necessarily work together. The idea that a platform does not stand in the shoes of its users as a speaker does not exist just because evaluating a large volume of content is hard; it also accounts for the fact that the content moderation choices that the platform makes under (c)(2) can always be accused of inconsistency, and cited as evidence that the platform is speaking, not merely moderating users’ speech.

It is certainly possible for platforms to speak under the pretext of moderation: in an extreme example, a platform that “moderated” a user comment by removing the word “not” from a user’s post would seem to be the platform creating a completely different message, and thus speaking for itself. However, the vast majority of the time, a platform is not trying to stand in the shoes of its users, but ensure that its community operates under a common set of rules or standards: a neighborhood discussion board might disallow national political debates, a sports blog devoted to one team might exclude its rival’s fans, or an online encyclopedia might prohibit dictionary-style entries.

Should the many concerns about online content suggest changes to Section 230, the law must still permit this type of flexibility in content moderation, allowing websites, forums, and other content platforms to set their own boundaries for content that will be more restrictive and more focused than what the First Amendment requires the state to permit in the public square. Decisions about online content moderation are made far more often and must be made more quickly than constitutional

¹ Tarleton Gillespie, *Custodians of the Internet* 6 (2018).



litigation, and platforms developing their policies must have the space and ability to account for bad-faith users who attempt to game the platform's system as it develops.

Different Types of Moderation for Different Types of Harms

As we work to ensure a healthier online environment, the discussions include several different types of harmful content that can appear and spread online. It is crucial to recognize that the differences in these types of content, and the differences in how they cause harm, require that different content moderation strategies apply to each.

For instance, certain types of illegal and harmful content can be definitively identified, fingerprinted, and found if they appear again. Specific files that contain child sexual abuse material (CSAM), for instance, can be identified if copies reappear. However, other types of online harm, such as messages representing stalking or harassment, are not represented by any specific files or strings of text. While both represent serious problems, the type of moderation appropriate for each is substantially different.

Matters can become even more complicated when dealing with other harms, such as terrorist content. While certain specific graphic files can be actively identified automatically, as with CSAM, a general prohibition against "terrorist content" raises many questions about defining terrorism today. Many authoritarian governments are quick to label protest as promoting terror, sedition, or the overthrow of a government; activist groups can be labeled as terrorist organizations by their political opponents. Platforms seeking to reduce the presence of terrorist content on their systems must make difficult judgment calls that cannot be made automatically.

Machine learning and artificial intelligence systems cannot solve many of these inherent ambiguities. Furthermore, the Foundation's experience with machine learning systems confirms that such systems are only as good as their training, which is based on data gathered by humans and is implemented by human annotators, who bring their own biases to the training of the systems. For instance, one recent paper found that a system designed to automatically detect hate speech was biased against African-American speakers.²

² Maarten Sap, Dallas Card, et al., "The Risk of Racial Bias in Hate Speech Detection," *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics* 1668 (2019).

Imagine a world in which every single human being can freely share in the sum of all knowledge.



Moderation of different types of harmful content also requires accounting for the balance of harms should the moderator make the wrong call. In some cases, a system that defaults to quick removal of suspected content is appropriate; in others, quick removal merely creates an easy way for bad faith actors to game the system and remove the speech of disfavored parties. For instance, consider a content moderation practice that removes a residential address that is suspected doxxing (the posting of a private individual's personal information in a way that threatens or creates harm). If the content is in fact harmful doxxing and is allowed to remain up, the harm to the doxxed user can be immense. If, however, the content is innocent but is removed by mistake or misidentification, the harm of that mistake is relatively small. This would suggest a policy that acts quickly on potential doxxing. In contrast, a policy regarding content that is reported for being defamatory could, if mistakenly left up, result in defamation being spread, but, if non-defamatory content is removed by mistake, could result in timely news reporting being suppressed. Policies incentivizing quick removal of suspected defamation could therefore cause more harm than good.

Recognizing the differences in how platforms can and should deal with different types of harms, however, cannot mean merely removing particular types of illegal, or even disfavored-but-legal content from the scope of Section 230. The ability for a platform to identify and deal with a particular piece of content has little to do with the severity of the harm it might cause and more to do with the type of information it is, and how it interacts with the platform. In the course of the 1.8 edits on Wikipedia made per second, any given edit could include a satirically false statement about a public figure, or an offer to sell drugs, but our volunteer moderators' or in-house staff's ability to locate these is the same, regardless of the scope of the potential harm.

Conclusion

Fostering a healthy online environment requires participation in good-faith content moderation on the part of platforms and their users, including moderation of content according to rules that are absent from the law--either because they represent difficult political judgment calls or because those laws would be unconstitutional. Section 230 currently allows that flexibility for rapidly evolving moderation and resists creating affirmative incentives for platforms to ignore problems. To the extent that policymakers and stakeholders want to create new incentives for increased moderation, we should take care that we do not incentivize platforms to take a path of least resistance that causes them to ignore mistakes in moderation or allow the gaming or subversion of moderation systems. As the Committee continues its exploration of these topics, the Wikimedia Foundation remains eager to answer any questions or assist in any way it can.

Imagine a world in which every single human being can freely share in the sum of all knowledge.

Before the House Committee on Energy & Commerce

**Subcommittees on
Communications & Technology
and
Consumer Protection & Commerce**

Hearing on:
“Fostering a Healthier Internet to Protect Consumers”

Oct. 16, 2019

Statement for the Record



MPA

AMERICA

Neil Fried
SVP & Senior Counsel
Motion Picture Association, Inc.
1600 Eye Street NW
Washington, D.C. 20006

At today's hearing on "Fostering a Healthier Internet to Protect Consumers," the House Energy and Commerce Committee will begin a reexamination of Section 230 of the Communications Act. When Congress originally passed Section 230 in 1996, its goals were twofold: 1) encouraging online platforms to proactively limit the availability of harmful content on their services; and 2) helping then-nascent online services grow, based on the belief they needed protection from liability for harmful content their users posted that they likely did not have the resources or technology to curtail. Although Section 230 does not shield platforms for copyright infringement by their users, Section 512 of the Copyright Act does, and was enacted in 1998 under a similar rationale as Section 230, while preserving some aspects of traditional secondary liability for intermediaries.

Critics of the online liability limitations argue that platforms are reaping the benefits of immunity without living up to Congress' expectations that they take reasonable steps to deter undesirable behavior. This is not an easy problem to solve, and we don't pretend to have all the answers. While the discussion is likely to be complex and involve a variety of proposals, the good news is that there are tools available today to begin addressing this issue while Congress conducts its reexamination.

Most internet intermediaries and user-generated content platforms reserve the right in their existing terms of service to remove unlawful or otherwise harmful content and to terminate the accounts of users who enlist their services for illegal activity. Calling on all online intermediaries and user-generated content platforms to take commercially reasonable steps to pro-actively enforce their policies regarding harmful and illegal conduct would go a long way toward curbing illicit activity online. Enforcing such policies could happen now, regardless of where the Committee's review leads. Moreover, companies can join forces with qualified private sector and public interest organizations that have raised concerns about harms stemming from third party content, and that can help craft effective tools and practices for addressing illegal activity.

For example, the MPA helps Visa, MasterCard, and PayPal identify pirate websites using their financial networks to profit off the mass, unauthorized distribution of entire movies and television episodes. Once identified, Visa, Mastercard, and PayPal can enforce their terms that prohibit use of their services to facilitate such activity, and terminate the accounts of wrongdoers. We similarly help Amazon, eBay, and Alibaba find sellers using their online marketplaces to peddle devices configured and marketed to access pirated content. We also work with Donuts and Radix, providers of newer top-level domains such as ".movie" and ".online," so that they can enforce their own rules against use of those domains for piracy. Trusted-notifier programs and other enforcement practices can help combat not just piracy, but a whole host of clearly illegal conduct.

A few companies have recently developed systems to proactively identify posts promoting hate and violence, and have invoked their terms of service to terminate accounts of those engaged in such activity, although not before wrestling with concerns over the impact on expression. If online intermediaries and user-generated content platforms can proactively identify such content and terminate service in these cases, surely they can terminate service and take other effective action in cases of clearly illegal conduct, which present brighter lines and don't raise the same speech concerns. Development and strong enforcement of such policies is

consistent not only with the original bargain of Section 230, but also with the claims of online companies that they should be allowed to self-regulate.

In the meantime, as Congress reexamines online liability limitations, the United States should refrain from including such limitations in future trade agreements, which runs the risk of freezing the current framework in place. Indeed, defenders of Section 230 have explicitly cited tying Congress' hands as one reason for including online liability limitations in trade agreements. Further, Congress did not include Section 230 in Trade Promotion Authority in 2015. We support the US-Mexico-Canada trade agreement because, on the whole, it improves on the copyright policies included in NAFTA, which was adopted prior to the internet age. But including online liability limitations in future trade agreements could usurp Congress' prerogatives. The United States should allow Congress' conversation to run its course before exporting the limitations, as well as the problems they may be exacerbating.

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge



GOOGLE

SEARCHING FOR HELP

She turned to Google for help getting sober. Then she had to escape a nightmare.

By [Cat Ferguson](#) | Sep 7, 2017, 8:00am EDT

Leasha Ali had been drunk for the last two days, but she didn't want to be anymore. The 39-year-old math teacher and mother of two was in a spiral familiar to anyone who's struggled with addiction. A difficult event — a hospitalization, thanks to lingering symptoms from a birth defect — had stressed her to the breaking point, and then she'd gotten home and found herself alone in her house, depressed and unable to sleep. After a few days without drinking, she gave in, and spent the next 48 hours on a bender.

On the second night, January 8th of this year, she got an email from the hospital. Her liver enzymes had been dangerously high — even before the days of abuse. The birth defect that put her in the hospital had already left her with several damaged organs. Afraid of hurting another, she searched the test results in Google. Right there at the top was an ad for rehab.

"I thought to myself, 'Oh my God, even Google knows I need rehab,'" Ali told me.

It's hard to say exactly who was on the other end, when, just before 11PM, Ali called the number in the ad. The 800 number was ephemeral. It's missing from Yellow Pages listings, social media, and even sites for complaints about telemarketers and spam, and it was disconnected by the time I called it. The untraceability is frustrating, but not surprising. Google offers advertisers unique "tracking" phone numbers that forward to a company's

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

phones, so they can understand which ads are bringing in the most clients. The phone numbers only stay up as long as the ad does.

"OH MY GOD, EVEN GOOGLE KNOWS I NEED REHAB."

Ali's call to the hotline lasted almost an hour. The woman asked for Ali's insurance details and other personal information, which Ali gave her, but mostly, they talked. Ali told the woman what was going on with her, why she wanted treatment, and what kind of rehab she hoped to end up at. "Somewhere with palm trees," she remembers requesting.

The woman told Ali she'd call back with a referral. Ali fell asleep while waiting.

KEY POINTS

- Google results for phrases like "rehabs near me," along with the resulting ads, are often peppered with 800 numbers for lead generators, third-party call centers selling potential clients to rehabs
- Some rehabs run hotlines that seem like unbiased referral services, but refer most patients to treatment centers they own
- The worst operations overbill insurance for tens of thousands of dollars, pay referrers a portion of the bill, and in extreme cases, can look a lot like human trafficking
- Deceptive practices are common in online rehab marketing, including Google and SEO scams that redirect callers away from legitimate treatment centers
- At some call centers, reps are paid bonuses for "performance" (i.e., how many admissions they sign up), and many use high-pressure sales tactics on desperate callers
- A new law in Florida, where many of the call centers are based, bans deceptive sales tactics for rehabs
- It remains unclear how much legislation and other pressures will affect these marketing practices

At 8:30AM the next day, her phone rang. It was a placement service called Aid in Recovery, and it'd found a good place for her, a Florida outfit called Wellness Counseling and Residential Detox.

"Our mission is to make sure you have the best possible chance to break free from alcohol and drug addiction. We do this by matching your specific needs with the best rehabs across the nation," Aid in Recovery's website promised when Ali looked it up. Spending January in Florida was an easy sell. At 12:30PM, Aid in Recovery sent Ali flight information. Four hours later, she was on a plane.

"I had a lot of guilt and shame about my drinking, and so I really wanted to stop. I'd been trying to cut back, and I realized I wasn't going to stop on my own," Ali told me over the phone a few months after she got out of Wellness. Had she been clearheaded, she thinks she might have noticed the warning signs, like the salespeople telling her that treatment wouldn't cost her anything.

What Ali found in Florida was a far cry from the tailored retreat she was expecting. The facility was in a recently converted ex-motel; she told me her room was crammed with three twin beds and a small chair. Most of her treatment at the understaffed facility consisted of large therapy groups, and personnel were unprepared to deal with her serious medical issues. Having started out looking for help with her alcoholism, she ended up getting a lesson on the complex, opaque web of treatment centers and marketing operations that use the internet and high-pressure telemarketing techniques to profit off a booming market: addicts in America.

In the shadow of America's opioid crisis, an array of business models have sprung up to generate "leads," marketer-speak for addicts with money — or good insurance. Some are

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

third-party marketers operating referral hotlines, while others are entities owned by and referring to a single rehab company. Some serve both purposes, referring to their own treatment centers and selling the callers they can't use. While quite a few treatment centers and marketers are honest and upfront, many others use deception and call-center scam tactics to get clients.

SOME SPEND HUGE SUMS TO SHOW UP IN THE SEARCHES OF DESPERATE PEOPLE WITH THE RIGHT INSURANCE

The companies are united by their dependence on Google, some of them spending huge sums on ads to show up in the searches of desperate people with the right insurance. Aid in Recovery, the company that sent Ali to Florida, spends over a million dollars a month on Google search ads for websites they own, according to an estimate by web ad analytics company SpyFu.

Florida has taken notice of the industry's marketing tactics. On June 26th, Governor Rick Scott **signed a long-awaited ban** on deceptive treatment center advertising that outlines specific disclosure requirements and cracks down on other questionable practices that have become common in the rehab industry. The bill, which explicitly covers misleading statements online, passed unanimously in both the Florida House and Senate.

As of **June 24th**, Aid in Recovery's website continued to imply it was an independent company, as it had when Ali went to Florida: "We have the most accurate and latest information on treatment programs available," Aid in Recovery said on the front page. "We do not promote any particular approach to addiction treatment, just high success rates."

HAD SHE BEEN CLEARHEADED, SHE THINKS SHE MIGHT HAVE NOTICED THE WARNING SIGNS

By July 9th, Aid in Recovery had changed its web copy, deleting all of the language suggesting they were independent, and adding a disclaimer that the company "is associated with affiliated treatment centers located in AZ, CA, and FL and Aid in Recovery may refer a person to one of these entities if the person's treatment needs and payment abilities match the treatment offerings at these facilities." (Aid in Recovery also removed some aggressive and misleading statements about going to rehab far from home, including that "it has been proven that the success rate is higher" when addicts go out of state for treatment.)

Some of their affiliates are now named on the website, including Wellness, where Ali went. But those aren't the only businesses in Aid in Recovery's network. Company filings and court records reveal a tangled web of holding companies within blandly named holding companies, adding up to a multimillion-dollar rehab business, all tied together by an LLC called **Treatment Management Company**. It spans four states, and includes phone rooms, urinalysis labs, detoxes, and rehabs. All of them are connected to one man, Bryan Deering, a millionaire who made his money in concrete.

Many are concerned about the way profits in the industry have been prioritized over patient outcomes. In 2015, Michael Lukens, a former business partner of Deering's, made a YouTube video denouncing unethical behavior in the rehab industry.

"I actually have perspective from behind the scenes," Lukens says on the video. "By and large, the mentality of the owner-operator is continuously putting profits ahead of people."

"We completely reject any suggestion that we have been deceptive in our operations or in dealing with clients or prospective patients," Treatment Management Company said in an

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

emailed statement. "Our marketing efforts are in line with other health care companies in the United States."



pen another tab, and Google "alcohol rehab near me." Take a look at the ads up top. (If you have an ad blocker, you'll have to turn it off.)

If you're in Arizona, and you click on the top ad, you'll cost that advertiser around \$221. If you're in Colorado, that click costs the site \$230. Sorry, New Yorkers, your click is only worth \$43 — but if you searched "drug treatment centers," you'd go for around \$121. (These are estimated averages from April this year, provided to *The Verge* by advertising analytics company SEMrush.)

That's assuming you don't live in a city with a high percentage of Medicaid recipients. In New Jersey, the statewide cost for ads on "best alcohol rehab centers" searches is \$190 per click, but that's an average. Smart marketers tell Google they don't want their ads showing up in any searches from Trenton, Camden, or other low-income cities. It's also good practice, if you're hoping to attract well-heeled (or at least well-insured) clients, to keep your ads away from searches with words like "free" and "Medicaid."

Of course, there are other ways to prevent poor people from calling your hotline. One of Aid in Recovery's AdWords listings, which I saw on Google in the middle of August when searching for "treatment center South Florida," is titled "Addiction Treatment Center - No Medicaid. No Medicare." When I repeated the search, their listing was titled "Addiction Treatment Center - (Private Insurance Only)." A few days later, I tried "texas rehab" and got an Aid in Recovery listing titled "Luxury Drug/Alc Rehab Centers. - (Private Insurance Only)." All three list different 800 numbers.

Some methods of targeting patients are more deceptive. My editor in New York City Googled "rehab" in February; one of the top AdWords results was for The Watershed. "Rehab in NY - Choose The Watershed Rehab," it read, listing an address in Brooklyn. "No Medicaid/Medicare." Searching the Brooklyn address brings up their "[locations](#)" page, which clarifies the rehab "provides treatment services only in our Florida and Texas facility locations," before listing addresses in 32 other states, including nine in New York and eight in New Jersey. (The other three ads in my editor's results were for rehabs in Florida.)

THAT CLICK COSTS THE SITE \$230

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

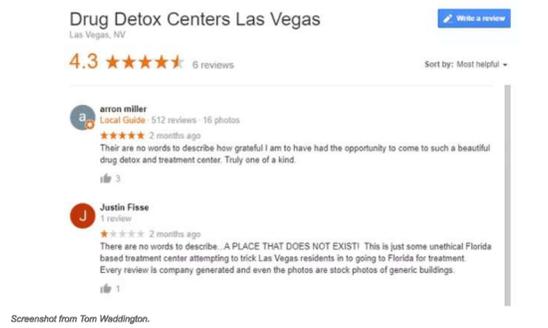
A friend Googling "rehab near me" in the Bay Area in August got ads for a third-party lead generator; a local rehab with a hotline that rang to the parent company's New Jersey call center; and a site operated by Aid in Recovery (its closest facility is 400 miles away).

Once a potential client is on the phone, it's up to the phone room salesperson to convince them that they should travel to the treatment center the call center is repping, whether or not going away from home was the person's intention.

"Google 'drug treatment Dayton Ohio,'" Alan Johnson, chief assistant state attorney of Florida, suggested to me. "Call a couple of those numbers that pop up, right up front, and see what you get." He laughed a little. "See if you actually get somebody in Dayton."

Johnson is head of the Palm Beach County Sober Homes Task Force, which has been helping draft legislation about fraud and other illegal activity in the treatment industry since July 2016.

Google declined to comment on the record when I asked them about issues around geographic targeting of ads.



The search giant actively courts treatment centers, both online and off. In May, a Google "digital ambassador" was a featured speaker at the [Treatment Center Executive & Marketing Retreat](#), a networking getaway for C-suiters and financiers of addiction treatment businesses. In July, two Google executives talked about AdWords at a [marketing conference for mental health professionals](#). And in February, *Addiction Professional*, the rehab industry's main trade rag, ran a webinar called "Attracting Patients Online in Their Time of Need." One of the speakers was Danielle Bulger, a senior account executive with Google's health care division and a featured speaker at the aforementioned retreat.

In a study using what Bulger called their "humongous dataset," Google found 61 percent of people who went to rehab used the internet to find treatment — a bigger number by far than those who relied on their family, friends, or doctors.

"While the gravity of the situation is not lost on us here at [Google], we do know that if we do our jobs well as marketers, as digital evangelists, as content producers that answer these very important questions, we can help lives," Bulger told her listeners.

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

"SEE IF YOU ACTUALLY GET SOMEBODY IN DAYTON."

But the search engine's ubiquity gives scammers easy access to the same customers, and their business-friendly tools work equally well for black- and white-hat marketing.

One of the most common scams is so easy you could try it yourself (but please don't). Google's business listings — the snippets that pop up in Google searches or on Maps — all have a little link in them: "Suggest an edit." If a business hasn't claimed its listing, it's easy to change the phone number to anything you want. Scam marketers do it constantly, rerouting a treatment center's calls to their own hotline, trusting their sales reps to convince the caller they've come to the right place, as Alfred Lubrano of the [Philadelphia Enquirer](#) reported in June.

Even if a company has claimed the listing for their center, which usually involves Google mailing a postcard with a security code to the business address, sometimes Google's algorithm lets spammers' suggested edits through anyway. Business owners aren't notified of such changes by email, instead seeing them only if they log into their "Google My Business" account page, according to Tom Waddington, a Google Top Contributor, which means he volunteers to answer user questions in the Google help forums. (In exchange, Google gives him easy ways to escalate reports about scams and other complaints to Google employees, and flies him to Mountain View every year for a special conference.)

"Overall, allowing users to suggest and moderate edits provides comprehensive and up-to-date info, but we recognize there may be occasional inaccuracies or bad edits suggested by users," a Google spokesperson told me via email. "When this happens, we do our best to address the issue as quickly as possible."

But experts told me it's a lot more common than Google suggests.

"If you're a facility and you don't check your map on a regular basis, you will be hijacked," cautioned Johnson. And patients need to be careful, too. Once the rep has you on the line, he says, they'll tell you whatever they need to to reel you in. If a patient is looking for a specific rehab, Johnson told me the reps might respond, "Well they're full, but we have the same program in Delray Beach." Like as not, they hook somebody in, thinking they're getting something that they're not getting.

"IF YOU'RE A FACILITY AND YOU DON'T CHECK YOUR MAP ON A REGULAR BASIS, YOU WILL BE HIJACKED."

Sam Bierman, executive director of Maryland Addiction Recovery Center, a strong [critic](#) of [shady marketing tactics](#), has a couple of quick and dirty rules for families and doctors on the hunt for a rehab. One is to pay attention to the website's staff page. If they don't list their top brass, at the very least, then you have no idea who you're talking to, and should consider looking elsewhere. He also suggests asking the person who answers the phone if they're actually at the treatment center. If they tell you they're based somewhere else, tread carefully.

A few weeks before we talked, a fake number showed up on the Google listing for a treatment center owned by a friend of his. Bierman gave it a call. "I said, 'Are you guys a treatment center?' 'No, we're a national hotline.' I said, 'Okay, well are you guys for-profit or not-for-profit?' And she said, 'No, we're a national hotline.'" Then the woman hung up on him.

"A lot of it is just taking advantage of consumers who may not know any better," Bierman told me with anger in his voice.

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

Google has made [efforts to block such hijacking](#), but it's a game of cat and mouse. When lead generators aren't hijacking real rehab listings, they're submitting dozens or hundreds of fake ones, spamming Google Maps in an effort to get their 800 number in searches for, say, "rehab Los Angeles." In the early days, a treatment center in Florida could give legitimacy to a fake listing just by renting a post office box to receive the security code. Google eventually got wise to that, so scammers switched to private mailbox rentals, people's houses, and "virtual office" services.

Scammers in other industries try to game AdWords and Google business listings, too. Google has to contend with lead generators for [locksmiths](#) and other businesses pretending to be a specific company near the searcher's location, and fraudsters have used AdWords for [phishing attempts](#), keylogging malware, and [tech support scams](#).

Some security experts complain that the company's response to scams, especially those using Google Maps business listings, is glacially slow. For instance, in 2014, security expert Bryan Seely hijacked the phone numbers on Google Maps business listings for [FBI and Secret Service](#) offices. A year later, when Google still hadn't fixed the security flaw, he used the same technique to create a verified Maps listing for Edward Snowden's office... inside the White House.

"A LOT OF IT IS JUST TAKING ADVANTAGE OF CONSUMERS WHO MAY NOT KNOW ANY BETTER."

Waddington told me he hasn't seen any complaints from rehabs in the Google help forums recently, but said complaints tend to come in waves. "Hopefully this current downtime is a sign that Google has improved their ability to combat the issue," he said, "but it could also just mean that drug rehab spammers have improved their ability to avoid detection. I feel Google has a long way to go in identifying and removing spam listings overall." He first saw complaints about business listing hijackings back in [February 2016](#).

Last year, Google trialed a more proactive approach, according to Mike Blumenthal, a Google top contributor and co-founder of Local U, a conference series on internet marketing. Google often gives him early information on [news about the search platform](#). Businesses in a few select demographics had to verify their location, or be hidden from search results. It was evidently too clunky. In July, a Google representative told Blumenthal they would instead be "leveraging a behind-the-scenes approach to combat" fraud, requiring less work from the business owner.

"We use automated systems to detect for spam and fraud, but we tend not to share details behind our processes so as not to tip off spammers or others with bad intent," the Google spokesperson told me by email. "We've significantly reduced fraud with treatment center listings on Google and are committed to continuing to eradicate this type of fraud on our platforms."

These kinds of rehab marketing techniques may seem like a uniquely modern phenomenon, but 16 years ago, the [Miami New Times](#) published a story that, anachronisms aside, could have been published today. Michelle, desperate to get sober, dialed the first rehab number in the phonebook. The salesperson quickly vetted her insurance, oversold the amenities, and bought her a plane ticket. When she landed, "Michelle discovered a few minor surprises: there was no fitness center, the pool was actually an algae-clogged hazard, and her insurance company was billed \$1,000 per day instead of \$400."

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

Like Ali, Michelle was searching at the height of desperation and latched onto whatever she saw first. In Michelle's case, the number popped up first in the Yellow Pages because the treatment center owner had filed the rehab under an alphabetically optimized name, Aaron Alcohol Abuse Addiction Assessment Counseling. (Business name paperwork took a pretty surreal turn during this analogue SEO war. In 2004, a former Sea Winds exec named his new company [AALCOHAAAAALA + A ABUSE 24 HOUR AAAA ABLE HEPLINE AND COUNSELING CENTER, INC](#); in 2011, The Watershed, the same treatment center juggernaut from my editor's Google search, registered to do business as the letter [A](#).)

ARTICLES OF INCORPORATION
In compliance with Chapter 607 and/or Chapter 621, F.S. (Profit)

ARTICLE I - NAME
The name of the corporation shall be *A Alcohol Abuse 24 Hour AAAA ABLE Helpline And Counseling Center, Inc.*

The internet opened the floodgates of opportunity for sketchy ad tactics. Since the mid-2000s, a hodgepodge of in-house and third-party marketers have been generating enormous call volumes via TV spots, radio ads, and thousands of carefully targeted websites.

Third-party lead generators often send out "raw" calls in a kind of roulette, ringing a few times at each contracted treatment center until someone picks up. Much more valuable is a "verification of benefits" call, forwarded from a phone room that pre-vets addicts' insurance policies.

Some companies are startlingly blunt in describing their services. Take Treatment Link, a shop out of Pompano Beach, Florida, which doesn't hide any details from prospective marketing clients.

THE WATERSHED REGISTERED TO DO BUSINESS AS THE LETTER A

"All of our leads are **exclusive, filtered, & HOT!**," they exclaim on a page titled "[Why We're #1](#)." They tout calls, generally [the most expensive in the industry](#), that are "qualified by our treatment specialists for cash payment or payment through an approved P.P.O network with [their insurance provider](#)."

Things are a little different over on Treatment Center Finder, the website Treatment Link uses to reel in addicts. "We provide treatment centers that guarantee your success," they promise — a pretty wild claim, considering the National Institute on Drug Abuse, part of the National Institutes of Health, [estimates that 40–60 percent](#) of addicts will relapse after rehab. "We will connect you with the drug rehab that will set you free from addiction, and lead you to a wonderful life beyond your dreams!"

Some call center practices, in particular paying per-head bonuses for each admission, risk turning into [patient brokering, essentially buying and selling patients](#). Common brokering practices include paying "junkie hunters" for clients; bribing patients with cash, drugs, and other incentives; and kicking back a portion of insurance reimbursements for blood, urine, or genetic testing. At its worst, patient brokering looks a lot like human trafficking, as addicts are [passed around between brokers, kept high, and even forced into prostitution](#). In Florida, [it can be](#) a first-degree felony carrying a \$500,000 fine.

After a few years of buildup, Obamacare kicked the scams into high gear. Suddenly, anyone could get insurance covering addiction treatment — including drug tests that, with

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

the help of a friendly medical professional, could turn one cup of urine into thousands of insurance dollars for rigorous chemical analyses. Professional groups generally recommend those tests only for confirming the results of suspicious or especially consequential pee-in-a-cup tests.

With exchange plans largely locked into paying for medically required tests, patients (and their urine) became gold mines. Some labs started offering kickbacks to treatment centers, who in turn began splitting the profits with halfway houses that would tempt clients with free rent and other services.

PATIENTS (AND THEIR URINE) BECAME GOLD MINES

More and more halfway houses and treatment centers opened, flooding the market with businesses [relying in large part](#) on trickle-down pee money. Street-level patient brokers and phone room lead generators stepped up to fill the beds with strategies across the ethical spectrum, including signing addicts up for Obamacare and paying their premiums. Some treatment center operators cut out the middleman by opening their own labs, which only increased the demand for new patients.

Almost every arrest by the Sober Homes Task Force has involved [urinalysis overbilling](#) in one way or another. "Laboratory testing as a complement to clinical care may be routinely billed for without legitimate proof of medical necessity," the task force wrote in a January report. "This is one of the engines that currently run the industry."

In 2007, web marketer Phil Cory started TreatmentUSA as a kind of Yellow Pages for addiction recovery businesses. When he added an 800 number eight months later, more than one provider offered him thousands of dollars if he would vet patients' insurance coverage ahead of time. He says he turned them down, sticking to selling raw calls off his 175 sites, and requiring centers to provide three appropriate phone numbers to people who didn't have good insurance or the money to pay. He later sold the company to rehab chain American Addiction Centers.

"THIS IS ONE OF THE ENGINES THAT CURRENTLY RUN THE INDUSTRY."

"I could have made millions — multimillions — off the calls I generated for the treatment industry playing the same game as anyone else, but I made pennies on the dollar sticking to raw calls," he told me wryly. "I went so far as to sell my company because the industry was getting horrific. There were bad actors coming into play and profiting ridiculously off of families, and that's just not right."

Cory and Johnson both say unethical marketers have made it incredibly hard for good providers to compete in the South Florida market. When your competitors are cheating, how do you stay honest and keep the door open? But now, they say, a reckoning has begun, and many treatment businesses are closing or fleeing the state.

"WHERE THERE'S HIGH ECONOMIC MOTIVATION, PEOPLE FIGURE OUT HOW TO SCAM GOOGLE."

Insurance companies have stopped paying out for urine tests the way they used to, stepped up audits, and delayed some [claims](#) to treatment providers. There have been over two dozen arrests of patient brokers in the [last year or so](#), based on investigations by a broad alliance of government agencies. The Sober Homes Task Force, where government officials are joined by industry stakeholders, has been helping push legislative change, such as this year's law banning deceptive rehab marketing, which will eventually require marketers to register with the Florida government.

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

"It really boils down to — tell the truth. Disclose who you are, what services you provide, where you are. And if people do that, they won't run afoul of the new law," Johnson told me.

But addicts and scammers are both renewable resources, and even a combination of state laws, high-profile arrests, and algorithmic tweaks can only go so far when there's money on the table and inventive cheaters to rake it in.

"The hackers have gotten better, Google's gotten better," Google blogger Blumenthal told me. "Where there's high economic motivation, people figure out how to scam Google."



When Ali clicked on Aid in Recovery's website, she found reassurance that their "knowledgeable and skilled admissions coordinators" would walk her through everything, and "create a customized treatment plan" just for her. "We do this by matching your specific needs with the best rehabs across the nation," the page said until the marketing bill was passed.

"The only thing they could say they did to match my needs was make sure the insurance would cover it," Ali told me.

Aid in Recovery employs clinicians, but the people who answer the phone generally aren't licensed medical professionals. One of their primary qualifications is often having lived with addiction themselves. Hiring addicts in recovery to sell rehabs (not to mention [antiques](#), [printer ink](#), [gold coins](#), and [fake timeshares](#)) makes a lot of sense for both parties. Heavy drug users tend to accumulate points against them in the job market, like tattoos, track marks, criminal records, and long gaps in their resumes. But the desperation of long-term addiction can hone a certain genius for persuasion, too — a valuable skillset in the sales world.

When Ali called, the woman who answered knew just what to say to get her onto a plane. "She talked about how I needed to do this for my family, and that waiting would only make it more likely that things would get worse," Ali told me. "I got scared."

"I GOT SCARED."

To get the hard sell myself, I tried Aid in Recovery's live chat a handful of times before the new marketing law, mostly asking about treatment for a heroin-addicted daughter. Asking for a list of treatment centers was a nonstarter, as was getting information about what kind of financial deals they have with the treatment centers. The more questions I asked, the

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

more aggressive the salespeople got. On one chat, the marketer told me her own mother had just overdosed on IV heroin and died, so she knew what I was going through. When that didn't sell me on giving her my personal information, she pulled out all the stops.

"I don't know what would stop you from wanting to speak with a specialist to get further information," she wrote. "The more paranoid you are the longer it's going to take to get your daughter the help she needs."

In their letter responding to my detailed questions, Treatment Management Company said, "At the time we started Aid in Recovery, we marketed it as an independent company since we often had to refer clients out for detoxification."

"Over time, we have developed a full service offering of medical detoxification services, residential treatment, outpatient services, after care services and limited toxicology services. Because we currently offer full treatment offerings and as state laws and regulations have evolved, we now disclose on our AIR website, and in our calls with patients, that AIR is affiliated with our treatment facilities."

The site does now say that they are affiliated with centers in Florida, Arizona, and California, and they'll say it on the phone, although they're much more cagey in the live chat. According to public records, Deering, the owner of Aid in Recovery, has started or purchased the following rehab brands: Treasure Coast Recovery, Wellness Counseling and Residential Detox, and Executive Recovery Center, also known as The Lukens Institute, in Florida; Mountainside Recovery Center, also known as West Coast Wellness Center, in California; and Serenity Care Centers, Red Rock Wellness Care Centers, and Red Rock Addiction & Treatment Company in Arizona.

BEFORE JULY, EVERYTHING ABOUT AID IN RECOVERY'S PRESENTATION SUGGESTED IT WAS AN UNBIASED REFERRAL SERVICE

He is also the owner of National Laboratories, which specializes in drug tests for rehabs. It's a legal arrangement — as long as they don't bill Medicare or Medicaid, both of which ban practitioners from referring to labs with the same owner, or to labs owned by a family member.

Treatment Management Company, according to a statement, provides administrative support, but does not control any of the companies.

Since the marketing bill passed, Aid in Recovery has toned down the aggressiveness of their website copy some, changing their ["in-state versus out of state" page to remove](#) both a statement about how a local treatment center can't prevent gossip or "people seeing who enters and leaves the facility," and the incorrect claim that "it has been proven that the success rate is higher when one receives their treatment from rehab out of state." (It may actually be worse, since [family participation](#) improves the likelihood you'll finish a given program.)

Before July, though, everything about Aid in Recovery's presentation suggested it was an unbiased referral service. Its employee email signatures, for example, had this disclaimer: "Aid in Recovery, LLC is a placement service...our advice does not constitute medical advice or diagnosis...substance abuse treatment services recommended by us are provided by independent treatment centers who are solely responsible for their content and for conformance with applicable [laws]."

I've reviewed a January copy of Wellness Counseling's guidelines for how employees should handle patient discharges. Although the email disclaimers stated that Aid in

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

Recovery wasn't responsible for the services provided to Ali, and that no one from the company was giving her medical advice, the policy tells a different story. (Emphasis theirs.)

"All admits' level of care and length of stay is [sic] predetermined by AIR and the [utilization review staff]...If a client leaves facility grounds (AWOL) and is gone for 2 hours or more, than the client shall be discharged. The client will need to call AIR and interview with the clinical director to be readmitted...If the client states he 'was promised' a shorter length of stay or alternate discharge plan, the case manager should call Aid in Recovery (AIR) **WITHOUT THE CLIENT PRESENT** and confirm the program commitment. If the patient committed to detox only or discharge to another facility outside of our system, then AIR will set up discharge plans with the client and coordinate transport. If the patient committed to a "full continuum of care", then the case manager will ask the AIR counselor that worked with the client to assist with convincing client to follow through on commitment."

I spoke with a second former patient of Wellness, who left after insisting he had been promised a shorter stay. The staff more or less followed the guidelines, he told me. The techs listened to his Aid in Recovery recording (although he was around to hear it), and once they heard him say he only wanted detox, they let him go.

"Physicians at Wellness Counseling and other treatment facilities make their own independent determinations regarding the appropriate treatment plan and length of stay," Treatment Management Company wrote in a statement. "Any statements to the contrary are false and defamatory."

Treatment Management Company has done a lot of growing up in the months since Ali called Aid in Recovery. Earlier this year, it expanded into Georgia, snagging a [17,000-square-foot office space](#), and this summer it finally got its own website, two years after getting a Florida business license. The site says the company has 31 treatment center locations across seven brands, and a "24/7 addiction hotline." No brand names are given.

When I asked a Treatment Management Company spokesperson how business practices have changed in response to legislation and the company's growth, he responded by email, saying, "A detailed timeline isn't possible. Internal policies, laws and regulations in three states have continually changed over the years. We have always been compliant with laws and regulations."

Deering got into rehabs in 2012, when he bought Treasure Coast Recovery, a rehab in Stuart, Florida. A year later, he bought a controlling interest in The Lukens Institute, a luxury rehab run by clinical psychologist Michael Lukens, and started Aid in Recovery to market them both. Multiple former employees who worked with Aid in Recovery independently told me Deering called clients "gold bars."

MULTIPLE FORMER EMPLOYEES SAID DEERING CALLED CLIENTS "GOLD BARS"

Asked about the "gold bars" comments, Treatment Management Company offered the following explanation: "The term 'gold bars' was invented by managers so that our phone reps understand that each person calling in is suffering from the ravages of addiction and needs to quickly get to treatment. Sadly, we sometimes spent hours getting approvals and we weren't always moving fast enough to get back to people who had their bags packed so they could start their journey to recovery. Managers urged our phone reps to think of each client as a 'gold bar' that we wouldn't let out of our sight until safe and sound – whether to one of our facilities or another facility where they could get the help they need."

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

Deering brought on Lindsay Lohan's press-hungry father, Michael Lohan, to market his new companies. "Inspired by his faith, Michael Lohan has decided to open the nation's first faith based clinical treatment center," a Lukens Institute [press release](#) said at the time. It was the second time God called to Lohan; in 2010, he claimed he was moving to Los Angeles to start a faith-based rehab, as well.

Lohan's press strategy for Aid in Recovery seems to have been centered around trashy headlines, including telling tabloids he wished [his daughter](#) would go to the Lukens Institute. [Teen Mom star Farrah Abraham](#) also went to the rehab, as did the "Tan Mom" [Patricia Krentcil](#). All three D-listers were [reportedly](#) repped by PR agent Gina Rodríguez, who didn't respond to a request for comment. Treatment Management Company told me no patients have ever been paid to go to one of their rehabs.

In late 2014, Lohan, who has also worked with several [treatment centers](#) in South Florida unaffiliated with Deering or Treatment Management Company, told [Radar](#) he was fed up with crime in the South Florida recovery scene. "Such treatment centers turn a person's dream into a nightmare," he reportedly told the gossip rag.

Lukens left the company right around when [Radar](#) published that story, because of what he calls "philosophical, moral, and ethical differences between us." He told me that patients would regularly come to the Lukens Institute and say someone in the phone room had lied to them about the program and its offerings. "Nobody said, 'Bryan told us to lie,' but I went to him about it and complained, and it didn't stop. So, he was either unable or unwilling to stop it," Lukens said.

"HE WAS EITHER UNABLE OR UNWILLING TO STOP IT."

According to Lukens, he made a deal that Deering would buy out his stake over the course of two years and then stop using The Lukens Institute name, which Lukens has trademarked. The psychologist maintains the deal has not been honored. "I took my toys and tried to go home, and he kept some of my toys," Lukens told me.

When I called the number on The Lukens Institute website, the answering service still said "Welcome to the Lukens Institute." When I pressed three for the clinical director, I got the voicemail for Executive Recovery's director, and when I pressed one for more information, I got Aid in Recovery, who told me their programs were "similar to Lukens, of course, but he has his own thing, mostly self-pay." The Lukens Institute logo appears on at least one Aid in Recovery website, as well. Treatment Management Company maintains the parting was "amicable" and that the purchase agreement allows for the use of the name.

About a year after leaving, Lukens made a [video echoing Lohan's sentiment](#), criticizing the industry at large, including the "unscrupulous and sometimes criminal activity" of some treatment center owners.

"I actually have perspective from behind the scenes — by and large, the mentality of the owner-operator is continuously putting profits ahead of people, so very little attention is paid to improving the quality of care over time. It's as if they realize there's no money in it," he deadpans, with a college professor's resigned irony.

"The FBI is quite interested in this industry, and they're looking to crack down on some of these practices, and I support that wholeheartedly — I hope they clean up some of the mess here."

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

PP told her my life story," Ali said of the woman who answered her first phone call. "She listened, and confirmed all my feelings, you know? She validated me." Ali says the rep told her it wouldn't cost anything out of pocket. She has yet to receive a bill from the company.

The salesperson took down Ali's insurance, and promised to call back. The next morning, an Aid in Recovery rep called to book her a flight to Wellness, a treatment center that matched her needs. Shortly after, she got an email asking her to confirm she could fly with her health conditions; once she'd sent that, she got an email with her flight information, which put her in Florida by dinner. She barely had time to pack.

SHE BARELY HAD TIME TO PACK

It's common for treatment centers in Florida to offer prospective leads inducements like plane tickets and waiver of co-pays and coinsurance, generally having patients sign a promissory note to pay them back. The notes theoretically prevent the plane tickets from being a violation of Florida's anti patient-brokering laws.

Although Ali's credit card was charged for her plane ticket, the other patient I spoke with had Aid in Recovery buy his ticket. He signed a promissory note, though he told me he didn't feel pressure to pay it back. According to former employees who worked with Aid in Recovery in its first two years, phone room salespeople were paid monthly performance bonuses. One told me they were paid based both on how many patients they brought in, and on other metrics, such as convincing patients to pay for their own flights.

(A recent job listing for Aid in Recovery lists the following responsibilities: "Sell a certain program based on the insurance, available resources, age, gender, and medical needs...Be prepared to ask client if they're able to contribute any money for either their flight, money on top of an insurance policy or to pay an out of pocket expense...Transfer the client to a client care coordinator to book a flight.")

Both patients feel Aid in Recovery over-promised what Wellness offered. They both spent about a week in detox and then moved to the rehab, a motel that had been converted a month or two before. The patients were co-ed, ranging from teenagers to the elderly. Ali and the other patient told me they were at Wellness with an old man with diabetes and a walker. They also told me people with widely divergent needs were mostly treated through group therapy sessions.

THEY DESCRIBED THE ATMOSPHERE AT WELLNESS AS DISORGANIZED AND UNDERSTAFFED

The two patients I spoke with described the atmosphere at Wellness as disorganized and understaffed, having just opened a few weeks before. Shortly before the man left, the treatment center sent a large group of people to the Executive Recovery Center, which does intensive outpatient while putting clients up in sober living houses. The patient, who told me his only drug use was alcohol, stayed behind, eager to get out of there.

"I learned about more drugs than I'd ever learned about in my life," he told me. "The people that were doing drugs were *chain* smoking. They said they were smoking about five times what they normally smoked, because there was nothing to do." While he told me he wants the company to be held accountable for their deception, he wasn't comfortable publicly discussing his stint in rehab, so I agreed not to use his name.

Individual therapy wasn't much better. Ali wasn't sure the center assigned therapists at all; the man thought he *had* an assigned therapist, he just wasn't sure who it was. Several

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

therapists talked to him during his time there, he recalls, mostly finding him on the outside patio and joining him for a chat.

"I LEARNED ABOUT MORE DRUGS THAN I'D EVER LEARNED ABOUT IN MY LIFE."

"They'd just did it nonchalantly, it wasn't like they called us into a room and talked to us," he told me. Walking up to someone in a public area and asking how they're doing is not a standard therapeutic technique.

"The center meets and exceeds all staff to patient ratios set by the state of Florida," Treatment Management Company said in their statement. "Counseling sessions – individual and group – are provided [in detox] but the focus in these critical early days of recovery is on treating the physical symptoms of withdrawal."

Ali's insurance was charged significant amounts for urinalysis throughout her stay. Three times — Ali's first and last days in detox, and her second day in the rehab facility — Wellness Counseling and Detox billed her insurance \$3,615 for a urine test, while [National Laboratories](#), owned by Deering, billed her insurance \$6,800 for so-called definitive testing of at least eight drugs. Medicare rates for the tests are \$79.81 and \$155.42, respectively.

ALI'S INSURANCE WAS BILLED \$74,785 FOR 11 DAYS

In total, between Wellness, National Laboratories, and the medical providers who billed separately, Ali's insurance was billed \$74,785 for 11 days: \$40,605 for four days in detox, and \$34,180 for a week in the residential treatment center. Her insurance company reimbursed them \$22,046.37, about a third of what the providers requested, according to Ali's explanations of benefits.

"The [drug] test done at Wellness upon admission provides limited information to begin treatment, and comes back within a couple of hours. If the doctor needs more detailed information on the exact drugs and levels in the patient's system, he orders a confirmation test at National Laboratories," Treatment Management Company said, referring to their general practices, which are not illegal.



Ali had been at Wellness Counseling for about a week when she got sick.

Ali has gastroschisis, a rare birth defect involving the intestines and, often, other organs. She has to be careful about what she eats, has an implanted defibrillator, and regularly spends time in the ER for painful, even life-threatening abdominal problems.

Wellness Counseling doesn't have an on-site doctor, and Florida doesn't require them to, although the Sober Homes Task Force bill instructs the Department of Children and Families (DCF) to draft stiffer regulations by the beginning of 2018. Wellness' medical director, [Jeffrey Bishop](#), is an osteopathic physician who uses his internet presence to shill for a multi-level marketing company that sells "Natural Weight Management Coffee...Also a very effective Immune Drink." Medical care was provided by a nurse practitioner who came to Wellness once a day.

On January 20th, Ali told staff that she was having stomach pain. One staff member suggested a painkiller that would have made the situation more dangerous, according to Ali. Upset by the interaction, she went back to her room. Then she realized she was having a medical emergency and went back to the front office for help, but was told she would have to wait.

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

SHE BEGAN DEMANDING A PHONE TO CALL 911

Increasingly anxious about her pain, she began demanding a phone to call 911, she recalls, but no one would let her use one. Several hours after her symptoms began, the staff finally called her an ambulance.

When she finally got to the hospital on Saturday night, she was determined not to end up back at Wellness. Thankfully, she didn't require major medical intervention, and convinced her discharge nurse to refer her to another treatment center, but their admissions office was closed until Monday. Exhausted, miserable, angry, and alone, not sure where she was, and with all her money and clothes back at the rehab, she picked a random direction and started walking.

She happened to walk by the sheriff's station, where a deputy agreed to help her retrieve her belongings. After several hours of chaos and frustration at Wellness, she got some of her stuff, including her cellphone and enough money to buy a plane ticket, and called a car to take her to the airport, she recalls. But the staff gave her something else by accident: the guidelines for staff members discharging patients. That was the first time she found out Aid in Recovery was more than just a referral company.

SHE PICKED A RANDOM DIRECTION AND STARTED WALKING

"When I saw the name Aid in Recovery on that paperwork, it shocked me," she said. Back home in Texas, Ali began looking into the company.

She contacted every local, state, and federal agency she could think of, but it didn't do much good. She filed three reports with the Department of Children and Families, which polices treatment centers in Florida, but each time, they would immediately close the case, she recalls. It wasn't until she complained to the Office of the Inspector General that DCF undertook a formal investigation.

An inspector visited the site, spoke to one patient, several Treatment Management Company executives, and reviewed a variety of documents, including Ali's medical records. She determined there was no wrongdoing by Wellness in a report that referred to the treatment center as "Wellington Counseling & Residential Detoxification Services" throughout.

DCF is, according to both people in the industry and in law enforcement, underfunded and otherwise ill-equipped to police thousands of treatment centers and halfway houses. A December grand jury report found the agency had [25 licensing specialists for 931](#) licensed rehabs. And until the last legislative session, which ended in May, they barely had the ability to punish treatment centers operating without a license, let alone those that break some rules and stick to others.

As of July 1st, the agency is getting more cash from licensing fees, and has the power to immediately suspend a treatment center's license. Operating without a license is now a third-degree felony, and background checks are now required for owners, directors, and clinical supervisors.

"WHEN I SAW THE NAME AID IN RECOVERY ON THAT PAPERWORK, IT SHOCKED ME."

These changes come after years of media and community pressure to clean up the industry. The Sober Homes Task Force finally broke legal ground late last year, with the first [arrests of treatment center owners and operators](#) who were allegedly involved in patient

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

brokering schemes. Dozens more have since been arrested, [around a quarter of whom have pled guilty](#).

The Task Force also wrote most of the language in the deceptive marketing bill, which requires marketers to register with the state and creates penalties for lying about treatment programs. Johnson, state attorney and head of the task force, said the deadline and many of the details are still up in the air, but the [application](#) gives a sense of the scope. Marketing companies will have to give a full accounting of parent and holding companies, subsidiaries, and associated corporations, as well as a complete list of owners, business partners, trustees, shareholders, officers, and office managers, so the state can run background checks looking for fraud, embezzlement, and other relevant felonies.

Both of the bill's sponsors believe explicitly banning many of the tricks marketers use to lure addicts to Florida will result in fewer patients coming in from out of state. That's a big deal, considering approximately 75 percent of the current patient population in South Florida is from elsewhere.

Although this is movement in the right direction, Johnson had a word of caution about the law's reach. "These are guidelines," he told me. "It's up to the state and the industry to police ... The goal is to get back to an equilibrium where there's good treatment, as opposed to these rogue operators."

Ali, at least, found the treatment she needed, back home in Texas. She got a referral to a local treatment center from her psychiatrist — she's learned her lesson about calling numbers on the internet — and completed two back-to-back recovery programs. She's still sober, and now has to learn to navigate the world as an addict in recovery, with all the stigma that entails.

"I now belong to a different community of people, who don't have the same protection — that nobody fights for," Ali told me.

Laws may be changing, and a market correction may be underway, but that means more pressure and less money in an already oversaturated industry. "The next 18 months is gonna be the telltale sign," Cory, who started TreatmentUSA, told me. "You're going to see a lot of these [rehabs], especially in South Florida and California, shut their doors because they're not profitable."

SIZE DOESN'T MAKE A COMPANY IMMUNE TO THE INDUSTRY'S TARNISH

At the same time, treatment center conglomerates are [growing more and more common](#), taking advantage of the fiscal benefits of efficient, centralized decision-making and resource-sharing. But size [doesn't make a company immune to the industry's tarnish](#). Two of the largest rehab groups in the country — Elements Behavioral Health and American Addiction Centers — have been accused of unethical behavior, including hiring scammy marketing companies to steal Google [business listings](#), though both disavowed the marketers' actions.

Subsidiaries of both [Elements](#) and [AAC](#) have been accused of participating in urine test kickback schemes, while facilities owned by [AAC](#) and two other chains, [CRC Health Group](#) and [Recovery Centers of America](#), have been accused of maintaining lax standards of care that contributed to patient deaths. Former call center employees at the AAC facility told the *LA Times* [the sales environment was high-pressure](#), and all about getting heads in beds. Several staff members, including the former president of AAC, were indicted on murder charges, later dismissed.

10/15/2019

How disreputable rehabs game Google to profit off patients - The Verge

All four companies denied or failed to respond to journalists' questions about the above allegations.

At the moment, conglomerates control just a small part of the US market, but industry observers predict a steady increase in consolidation. All that money seems to be bringing with it a new kind of smooth-talking salesman: pharmaceutical reps.

"A lot of these venture capital firms are coming in and buying percentages, or whole treatment centers, and changing the salesforce from the marketing call centers into a pharmaceutical salesforce," Bierman, executive director of Maryland Addiction Recovery Center, told me. "We had a guy in our office a month ago, and I asked him what he did before this. He said he sold Viagra." ■

SCIENCE

With more rocket launches comes more cleanup

SCIENCE

Next year, new space missions will test technologies to fix busted satellites in orbit

SCIENCE

Stratolaunch, which built the world's largest plane, is changing ownership

[View all stories in Science](#)



SUBMITTED STATEMENT FOR THE RECORD OF

JEFFREY WESTLING
FELLOW, TECHNOLOGY AND INNOVATION
R STREET INSTITUTE

KRISTEN NYMAN
GOVERNMENT AFFAIRS SPECIALIST, TECHNOLOGY AND INNOVATION
R STREET INSTITUTE

SHOSHANA WEISSMANN
FELLOW & SENIOR MANAGER FOR DIGITAL MEDIA
R STREET INSTITUTE

BEFORE THE
HOUSE OF REPRESENTATIVES COMMUNICATIONS AND TECHNOLOGY AND
CONSUMER PROTECTION AND COMMERCE SUBCOMMITTEES
OF THE
ENERGY AND COMMERCE COMMITTEE

HEARING ON
FOSTERING A HEALTHIER INTERNET TO PROTECT CONSUMERS
SECTION 230 OF THE COMMUNICATIONS DECENCY ACT

OCTOBER 16, 2019

CHAIRMAN DOYLE, CHAIRWOMAN SCHAKOWSKY, RANKING MEMBERS LATTA AND
MCMORRIS RODGERS, AND MEMBERS OF THE COMMITTEE:

Thank you for holding this important hearing on fostering a healthier Internet to protect consumers and Section 230 of the Communications Decency Act. This statement is offered by scholars at the R Street Institute who have studied Section 230 extensively.¹

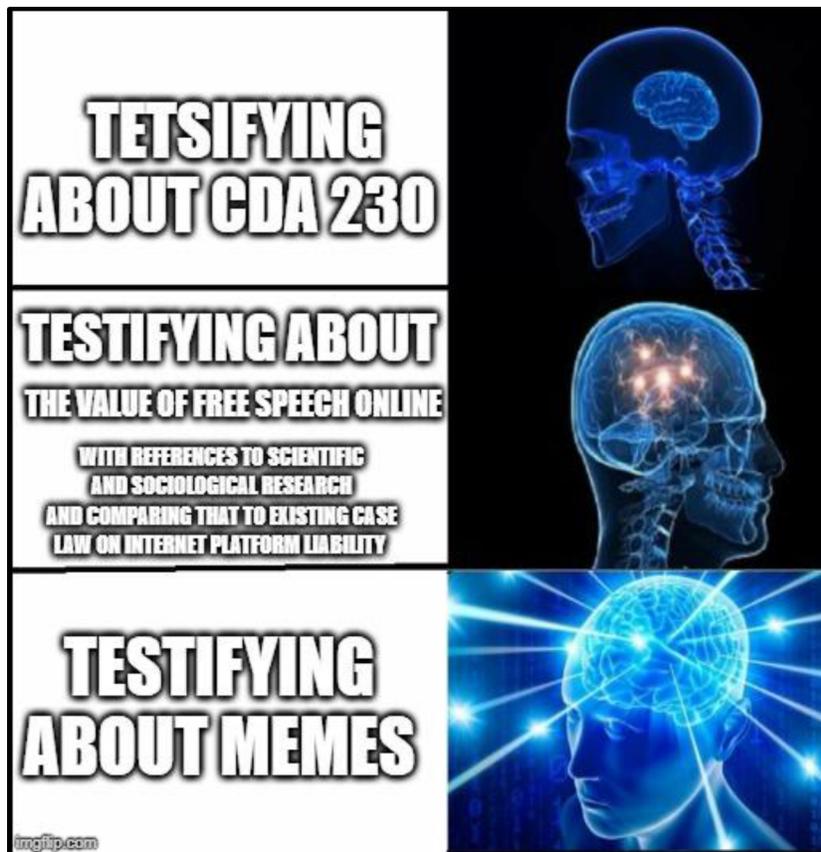
A hearing about Section 230 is necessarily a hearing about speech on the Internet. That topic is critical as the Supreme Court recognized in *Reno v. ACLU*, when it described the free speech capacity of "the vast democratic forums of the Internet."² But it is often difficult to perceive that capacity in the abstract.

So in an effort to make it more concrete, this testimony focuses on one idiosyncratic form of online speech, one that has taken the Internet and the culture at large by storm over a very short number of years, one that is immediately recognizable to all, one that is chided by some yet loved by many, one used by those of all walks of life from the high school freshman to the United States Government: the Internet meme.³

¹ The R Street Institute is a nonprofit, nonpartisan public policy research organization, whose mission is to engage in policy research and outreach to promote free markets and limited, effective government. R Street has written significantly on content moderation and Section 230. *See, e.g.*, Mike Godwin, SPLINTERS OF OUR DISCONTENT: HOW TO FIX SOCIAL MEDIA AND DEMOCRACY WITHOUT BREAKING THEM (2019); Jeffrey Westling, Submitted Statement for the Record, "Hearing on National Security Challenges of Artificial Intelligence, Manipulated Media, and Deepfakes Before the Permanent Select Committee on Intelligence," June 13, 2019, <https://www.rstreet.org/2019/06/13/testimony-on-deepfakes-before-the-house-permanent-select-committee-on-intelligence/>; Daisy Soderberg Rivkin, "Holding the Technology Industry Hostage," *The Washington Times*, July 1, 2019, <https://www.washingtontimes.com/news/2019/jul/1/the-stop-internet-censorship-act-would-ironically-/>; Daisy Soderberg Rivkin, "How to Realistically Keep Kids Safe Online," *R Street Blog*, Aug. 1, 2019, <https://www.rstreet.org/2019/08/01/how-to-realistically-keep-kids-safe-online/>; Shoshana Weismann, "Senator Hawley Introduces the Gold Standard of Unserious Social Media Regulation," *R Street Blog*, Aug. 9, 2019, <https://www.rstreet.org/2019/08/02/senator-hawley-introduces-the-gold-standard-of-unserious-social-media-regulation/>.

² *Reno v. American Civil Liberties Union*, 521 U.S. 844, 868 (1997).

³ Added original content. Original image retrieved from: <https://imgflip.com/i/3cxz0t>



The Speech Value of Internet Memes

While the term “meme” can refer to a wide variety of concepts, the most colloquially understood form of meme is the image-based visual meme. These memes have grown tremendously popular because of their relative simplicity, allowing users to take an existing idea and morph it to convey a new one.⁴ Social media also allows memes to spread at breakneck speeds to people across the world, further increasing their popularity as more individuals see and share

⁴ James Grimmelmann, “The Platform is the Message,” *Cornell Law School Research Paper No. 18-30*, March 1, 2018, p. 8. https://papers.ssm.com/sol3/papers.cfm?abstract_id=3132758.

them.⁵ As they spread, memes can become an entire body of communication among individual users who contribute new variations upon a meme that continues to change as the image spreads.⁶

To understand how this works in practice, consider the meme known as the “socially awkward penguin.” The base format is simply a penguin on a blue background, with captions above and below—but on that canvas users can relay embarrassing stories from their lives.⁷ While humorous, these images also are a way of letting out frustration and gaining a sympathetic ear from strangers across the world.



As a meme format becomes more popular, it evolves and mutates to convey new ideas. The “socially awkward penguin,” with only an image flip and a background color change, became the “socially awesome penguin,” allowing users to share life’s little victories.⁹ Consider the two memes below, which to a layperson appear nearly identical, but to those knowing that the blue image indicated awkwardness and the red confidence, understand them to be completely different.

⁵ Ibid.

⁶ Stacey Lantagne, “Famous on the Internet: The Spectrum of Internet Memes and the Legal Challenge of Evolving Methods of Communications,” April 1, 2017, p. 4.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2944804.

⁷ Ibid at p. 5.

⁸ Caitlin Dewey, “How copyright is killing your favorite memes,” *The Washington Post*, Sept. 9, 2015.
<https://www.washingtonpost.com/news/the-intersect/wp/2015/09/08/how-copyright-is-killing-your-favorite-memes/>.

⁹ Ibid.



The last major evolution of the meme came with a combination of the two, allowing the creator to tell stories of turning a socially awkward situation into a socially awesome one. Juxtaposing the two penguin memes above, as one insightful Internet denizen did, tells a remarkable story of self-esteem and personal gumption, entirely through a shared understanding of a seemingly meaningless graphic.¹¹

Clearly, memes are not mere images; they are a method of communication. They allow individuals to condense complex topics into simple formats and share these thoughts with others across the globe. More importantly, they create connections between these individuals and form communities that otherwise would be drowned out by larger interests. As Harvard professor Jonathan Zittrain explained, “A meme at its best exposes a truth about something, and in its versatility allows that truth to be captured and applied in new situations. So far, the most successful memes have been deployed by people without a megaphone against institutions that often dominate mainstream culture.”¹²

This innovative mode of communication can lead to both significant benefits and potential harms for users online. In a survey study on the impact of social media among teenagers, a Harvard Graduate School of Education researcher found that the vast majority felt empowered sharing their

¹⁰ /u/honorarymancunian, “It’s all about context,” *Reddit*, Oct. 29, 2011. https://www.reddit.com/r/AdviceAnimals/comments/lt6nm/its_all_about_context/

¹¹ Ibid.

¹² Jonathan Zittrain, “Reflections on Internet Culture,” *Journal of Visual Culture* 13:3, Dec. 16, 2014, p. 389.

identity through social media.¹³ Those surveyed indicated that they utilize various platforms for self-expression, personal development and growth, relational interactions and exploration.¹⁴ And while a spectrum of positive and negative feelings were experienced, the positive reactions tended to outweigh the negative.¹⁵ The study thus simultaneously confirms the communicative power that social media platforms can have and highlights the potential harms of social media, noting the presence of harmful content as a particularly difficult challenge.¹⁶

Memes also serve as visual tools used to critique expression, movements and popular online culture.¹⁷ A 2014 study looked at popular usage of “emoticons,” the small graphics used in short messaging services to convey anything from smiles to sadness (essentially a small-format meme).¹⁸ Among the reasons for emoticon use were to “[i]mprove understanding of message (35 percent), [c]reate a better atmosphere (22.5 percent), and [shorten time spent] writing (18.8 percent).”¹⁹ These results strengthen the value of image-based communications and memes as an effective tool for communication.

It is not hard to find anecdotes about the communicative potential of memes. Individuals with chronic pain often face skepticism and misunderstanding from those who have no frame of reference for the issue. Unfortunately, for many of these people, finding some form of community or understanding can be challenging.²⁰ Memes present an opportunity for this community, allowing bloggers and users to share their daily challenges and create a place where others will listen and comfort. One such community, for example, has adopted the “fibromyalgia duck” as a mascot in a campaign of memes—originating offline in fact, from a fundraiser involving actual

¹³ Leah Shafer, “The Ups and Downs of Social Media,” *Usable Knowledge*, May 16, 2018. <https://www.gse.harvard.edu/news/uk/18/05/ups-and-downs-social-media>; Emily Weinstein, “The social media see-saw: Positive and negative influences on adolescents’ affective well-being,” *New Media & Society* 20:10, Feb. 21, 2018.

¹⁴ *Ibid.*

¹⁵ *Ibid.*

¹⁶ *Ibid.*; See also, “Perspectives on Harmful Speech Online: a collection of essays,” *Berkman Klein Center at Harvard University*, August 2017. https://cyber.harvard.edu/sites/cyber.harvard.edu/files/2017-08_harmfulspeech.pdf

¹⁷ Thov Reime, “Memes as Visual Tools for Precise Message Conveying,” *Norwegian University of Science and Technology*, 2015. <https://www.ntnu.no/documents/10401/1264435841/Design+Theory+Article+-+Final+Article+-+Thov+Reime.pdf/a5d150f3-4155-43d9-ad3e-b522d92886c2>.

¹⁸ Tae Woong Park, Si-Jung Kim, & Gene Lee, “A Study of Emoticon Use in Instant Messaging from Smartphone,” *Human Computer Interaction, Application and Services*, 2014. https://link.springer.com/chapter/10.1007/978-3-319-07227-2_16.

¹⁹ *Ibid.* at p. 9.

²⁰ Elena Gonzalez-Polledo, “Chronic Media Worlds: Social Media and the Problem of Pain,” *Social Media + Society*, January-March 2016, p. 7. <https://journals.sagepub.com/doi/pdf/10.1177/2056305116628887>.

rubber ducks²¹—helping to facilitate connection with each other and express to the world the nature of their condition.²²



As with the chronic pain community, memes present an opportunity for distinct but disparate communities that would be unlikely to form without the immense size of social networks. People searching for these communities can find a home in these online spaces, as one social anthropologist writes: “By their admission, many seek and find ‘a family,’ a place where others will listen, somewhere one can turn to even when other social worlds might be unavailable due to the often random, persistent, and unpredictable temporalities of pain.”²⁴

And this community feeling is not limited to medical problems: Communities are built around memes relating to a variety of topics such as specific gender identities, which have grown immensely on sites like Reddit.²⁵

²¹ “Where Did the Fibro Duck Idea Come From?”, *Fibromyalgia Action UK*, May 11, 2014, <http://www.finauk.org/latest-news-mainmenu-2/articles-1/38-fundraising-1/910-where-did-the-fibro-duck-idea-come-from>.

²² Gonzalez-Piledo, supra note 20, p. 7.

²³ Ibid.

²⁴ Ibid.

²⁵ Heather Dockray, “The trans meme community on Reddit is about so much more than jokes,” *Mashable*, Mar. 15, 2019. <https://mashable.com/article/trans-meme-subreddits/>.

Memes can also convey public service information. In Utah, researchers developed an online campaign utilizing memes to promote healthy family meals.²⁶ With cuts to funding, researchers asked whether using memes and engaging with communities online presented an opportunity to reach these audiences.²⁷ While not definitive, the results of the project indicate the potential efficacy of such an approach.²⁸

In the field of policy, memes are a crucial form of advocacy, connecting with supporters, engaging bipartisanship and achieving policy goals. Indeed, our organization, the R Street Institute, frequently uses memes to amplify its perspectives and resonate with an ever-increasing online audience. Congressman Tim Ryan retweeted an R Street GIF supporting our stance on Congressional Research Service reform.²⁹ In this instance, the video meme connected a right-of-center think tank and a Democratic congressman on a policy issue.³⁰

Similarly, Senator Marco Rubio responded to an R Street tweet about lowering regulatory barriers for employees; dozens of others from varying political backgrounds commended him for it.³¹ Memes, in these instances, were effective in not only communicating a desired message clearly, but also in connecting opposed political groups.

Perhaps more importantly, in countries without strong democratic processes, memes have served as a tool to express dissent, akin to a public protest.³² Venezuela, for example, has restricted Internet access, removed content and blocked websites that promote criticism of the Maduro regime.³³ In order to subvert their attempts to remove protest content, many political dissidents have used memes, which are not as easily indexed by search algorithms (because they are images), to make it more difficult for the government to find and remove content.

Consider the following meme, which originated as a government photo to promote Maduro but ended as a vehicle for political criticism, with the added caption imagining Maduro pondering,

²⁶ Cameron Lister et. al., “The Laugh Model: Reframing and Rebranding Public Health Through Social Media,” *American Journal of Public Health* 105:11, Nov. 2015, pp. 2245-2251.

²⁷ Ibid.

²⁸ Ibid.

²⁹ Tim Ryan, @RepTimRyan, June 2019, [Twitter post] retrieved from <https://twitter.com/RepTimRyan/status/880491581970817025>.

³⁰ Ibid.

³¹ Marco Rubio, @SenRubioPress, April 2019, [Twitter post] retrieved from <https://twitter.com/SenRubioPress/status/1119254514996002819>

³² Heidi E. Huntington, “Subversive Memes: Internet Memes as a Form of Visual Rhetoric,” *Selected Papers of Internet Research* 14.0, 2013, p. 1.

³³ Kevin Gray, Manuel Rueda, and Tim Rogers, “Venezuelan memes reflect outrage and ridicule over president's desperation tour,” *Splinter News*, Jan. 2015. <https://splinternews.com/venezuelan-memes-reflect-outrage-and-ridicule-over-pres-1793844820>.

“Sometimes I think of returning to Venezuela / But then I remember how bad the situation is, and the feeling passes.”³⁴



35

To be sure, malicious actors can exploit this increased communicative power and virality of information to cause harm. Especially in the current era of disinformation, where individuals tend to trust and believe information that confirms preexisting beliefs and worldviews,³⁶ this predisposition to confirmation bias means that complexities are often lost in the wind. The emotional connections memes create between uncommon viewpoints can help underserved communities, but they can also enable tactics of persuasion that discard truth and nuance in favor of discord and faction. The simplicity of image-based memes, therefore, presents a unique opportunity for malicious actors to spread disinformation or hateful content online to individuals who will see the information, like it and continue its propagation.³⁷ The Internet Research Agency, for example, used memes as a way of dividing Americans during the runup to the 2016 elections.³⁸

What this potential harm highlights, however, is not a problem with image-based memes, but rather their effectiveness as a mode of communicating ideas. Even when faced with memes

³⁴ Ibid.

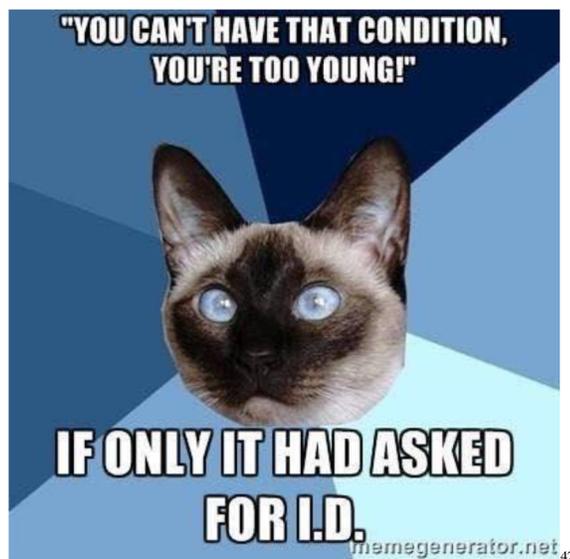
³⁵ Ibid.

³⁶ Jeffrey Westling, “Deception & Trust: A Deep Look At Deep Fakes,” *Techdirt*, Feb. 28, 2019. <https://www.techdirt.com/articles/20190215/10563541601/deception-trust-deep-look-deep-fakes.shtml>.

³⁷ Ibid.

³⁸ Nicholas Thompson & Issie Lapowsky, “How Russian Trolls Used Memes Warfare to Divide America,” *Wired*, Dec. 17, 2018. <https://www.wired.com/story/russia-ira-propaganda-senate-report/>.

that could be considered harmful, a community can use responsive memes to subvert that hateful or problematic speech. For example, some disabled communities find memes using their disabilities as a source of charity or inspiration problematic, devolving the individual into a simple stereotypes.³⁹ To combat this, these communities have begun using counter-memes, “taking the memes, turning the memes, planting other ideas in the memes and thus in society.”⁴⁰ This so-called “culture jamming” allows disabled people to “use as part of their own struggle to take control over their self-performance of disability, and the broader social performance of disability that contextualizes it.”⁴¹ In the following “Chronic Illness Cat” meme, for example, the creator lays out a common stereotype for a given condition, and pushes back on that idea with a snarky response.



This trend of using memes as a counter to harmful speech isn’t limited to any specific topic or demographic. Godwin’s Law—the famous “law” that states “[a]n online discussion grows longer, the probability of a comparison involving Nazi or Hitler approaches one”—is itself a meme

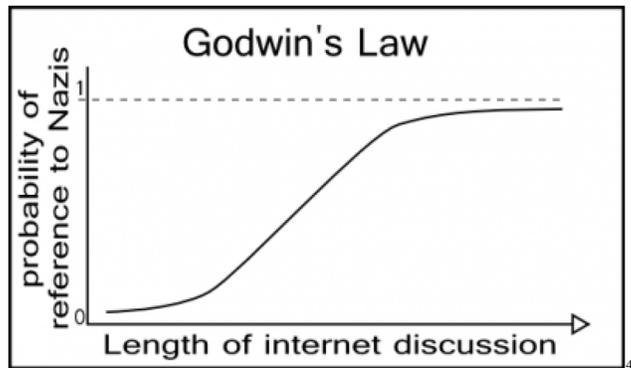
³⁹ Bree Hadley, “Cheats, charity cases, and inspirations: disrupting the circulation of disability-based memes online,” *Disability & Society* 31:5, 2019, p. 679.

⁴⁰ *Ibid* at p. 685.

⁴¹ *Ibid*.

⁴² Melissa McGlensey, “18 Memes That Nail What It’s Like to Live with Chronic Illness,” *The Mighty*, Oct. 25, 2015. <https://themighty.com/2015/10/best-chronic-illness-memes/>

(in the broader sense of a disseminatable slogan) designed to counter the so-called “Nazi-meme” of heated online discussion threads often devolving to name-calling.⁴³ As the creator himself explained in 1994, “[t]he best way to fight such memes is to craft counter-memes designed to put them in perspective.”⁴⁴



As a part of the online ecosystem of speech and content, then, memes represent essentially a form of innovation: a new way of communicating that takes advantage of an existing technological environment (one that supports easy sharing of images with wide communities at near-zero costs), giving users of this new, innovative practice an advantage in taking their messages to the world. Like all innovations, it can be used for good and for harm. The questions, then, as with all new technologies, are whether policymakers who define the regulatory environment over memes should foster them and other innovative forms of speech, and how regulatory measures that affect the platforms on which memes live will affect this form of communication.

Lessons for Policy on Online Speech and Platforms

Based on the immense value that memes provide to a wide variety of citizens, it is our view that Congress should encourage the production and dissemination of memes as an opportunity for all communities to make their voices heard on the “vast democratic forums of the Internet.”⁴⁶ In

⁴³ Michele Knobel and Colin Lankshear, “Online Memes, Affinities, and Cultural Production,” *A NEW LITERACIES SAMPLER* (Peter Lang Publishing, Inc. 2007), p. 223.

⁴⁴ Mike Godwin, “Meme, Counter-meme,” *Wired*, Oct. 4, 1994, <https://www.wired.com/1994/10/godwin-if-2/>.

⁴⁵ Godwin’s Law Chart,” *Know Your Meme*, last visited Oct. 8, 2019, <https://knowyourmeme.com/photos/39090-godwins-law>.

⁴⁶ *Reno v. American Civil Liberties Union*, 521 U.S. 844, 868 (1997).

particular, there are three lessons that Congress should consider in any discussion of online speech or Section 230, lessons that are laid out below.

Content Moderation Policies Should Encourage Open Communication and Target Speech Designed to Silence

It is vital that platforms work to protect communities like those described above, as they try to find their voice through memes or other forms of speech. It has become far too common for bad actors to seek to stifle this speech by flooding platforms with hate speech and harassment. This is especially true on platforms that take few or no steps to moderate user content.

If, for example, Senator Hawley’s bill—which would remove CDA 230 protections from companies who are not political neutral⁴⁷— passes, platforms would need to carefully consider if removing harassing speech from one political viewpoint would make them biased in the eyes of the FTC.⁴⁸ Unfortunately, if trolls targeting a specific community tend to come from one politically ideology, moderators may choose not to remove hate speech or harassment out of a fear that it would open the entire platform up to liability,⁴⁹ avoiding any knowledge of the content generally requisite to findings of legal liability.⁵⁰ The government itself is largely hamstrung in its ability to protect these. As a result, these communities may never find the chance to gain a foothold and be drowned out by harassment and hate speech.

However, most platforms recognize this as well, and want to create an environment where their users feel safe to express themselves without fear of harassment. Indeed, many of the largest platforms have policies against this type of behavior so as to allow these communities to grow. As a part of Facebook’s community standards, for example, the company explains that “[w]e believe that all people are equal in dignity and rights. We expect that people will respect the dignity of others and not harass or degrade others.”⁵¹ Violations of this policy subject the content to removal and the user’s account to suspension.

This is exactly the type of environment intermediary liability should attempt to foster. Platforms should not fear liability for removing users’ posts that attempt to stifle speech and community online. With certainty that their moderation decisions won’t lead to liability for all the

⁴⁷ Ending Support for Internet Censorship Act, S. 1914, 116th Cong., June 19, 2019.

[https://www.congress.gov/bills/116th-congress/senate-bill/1914?q=%7B%22search%22%3A%5B%22internet+censorship%22%5D%7D&s=1&r=1](https://www.congress.gov/bills/116/congress/senate-bills/1914?q=%7B%22search%22%3A%5B%22internet+censorship%22%5D%7D&s=1&r=1).

⁴⁸ Daisy Soderberg Rivkin, “Holding the Technology Industry Hostage,” *The Washington Times*, July 1, 2019. <https://www.washingtontimes.com/news/2019/jul/1/the-stop-internet-censorship-act-would-ironically-/>.

⁴⁹ *Ibid.*

⁵⁰ Jeff Kosseff, *THE TWENTY-SIX WORDS THAT CREATED THE INTERNET* (Cornell University Press 2019), p. 56.

⁵¹ “Community Standards,” Facebook, last visited Oct. 10, 2019.

<https://www.facebook.com/communitystandards/>.

content their users post, platforms may freely remove these posts rather than become wastelands of toxic content. This balance fosters growth on the platform and free expression online. Lawmakers should carefully consider how any shift in the law may stifle these voices.

Platforms Should Have the Flexibility to Allow Controversial yet Legal Content to Remain Online

An essential component of this debate is that what is controversial or inappropriate to some may not necessarily be controversial to others. While this may seem like a simple idea, in practice it can be hard to remember. Platforms should be encouraged to not over remove some user content just because it could be considered an offense to some.

Again, intermediary liability law plays a major role here. At the other end of the “moderator’s dilemma,” rather than leaving up all content to avoid potential liability, platforms may choose to over-remove content, silencing any voices that may possibly offend other users who could in turn sue the platforms for removal. This means that communities around controversial topics could find a significant portion of their content removed by moderators, effectively stifling their speech on these platforms.

Take, for example, the discussion of Venezuela above. Platforms may see this type of content shared within communities who disagree with the actions of the Venezuelan government potentially problematic, and even outside of Venezuela remove the content if they could face a potential lawsuit, justified or not. Rather than silence these voices, platforms should feel secure enough to allow users to share such posts and voice their opinions.

This isn’t merely hypothetical. Look at the recent actions by companies who fear retribution for their employees showing support for the protests in Hong Kong. Without wading into the debate, what this clearly shows is a different cultural understanding of what type of content is offensive and what is not. China’s state TV went as far as to say that “[w]e believe that any speech that challenges national sovereignty and social stability is not within the scope of freedom of speech.”⁵² This obviously contradicts the American understanding of free speech, but it also highlights that what should and should not be removed is ultimately a subjective question, and the wrong answer can and will stifle beneficial speech online.

Also, to the extent that platforms leave disinformation up, memes can potentially serve as a rapid response strategy due to their virality and mutational nature. If a book was published with disinformation, it would take the literary press some time to discredit it, while online rants can be discredited within minutes.

⁵² Arjun Kharpal, “China state TV suspends NBA broadcasts after Morey Hong Kong tweet,” CNBC, Oct. 10, 2019. <https://www.cnbc.com/2019/10/08/china-state-tv-suspends-nba-broadcasts-after-morey-hong-kong-tweet.html>.

Ultimately, many users will disagree about whether specific content is controversial and will seek to silence speech they disagree with. Without protections from liability, platforms will face a stronger incentive to simply remove the controversial posts even if such content is not patently offensive to many. Therefore, it is critical that intermediary liability protections allow platforms to not cave to the values of the few and over-remove content.

Platforms Should Have the Flexibility to Remove Truly Offensive Content

Despite the immense benefits that memes and speech online can provide, there are undoubtedly times in which content should be removed. Some of this content would break Federal law or violate intellectual property rights.⁵³ However, much of this content is not necessarily illegal, such as blatant disinformation and violent content. While intermediary liability law should encourage platforms to allow controversial posts to remain on the website, it should also allow the companies to remove content that violates platforms' particular standards of conduct.

An intermediary liability regime that allows companies flexibility and freedom to moderate as they see fit in turn leads to competition among services. As explained above, values differ greatly among different individuals. Some users will no longer use certain platforms if disinformation or violent content remains. At the same time, other users may not stay on a platform if information is removed that they believe to be true or otherwise do not find objectionable. Therefore, if one platform decides to remove content, users who wish to see that content will likely have other places to go and share their ideas. This is a good thing.

This market-based approach allows companies to find a balance that serves their needs without impeding free speech online. Instead of a few companies with similar policies, users can go to a multitude of different sites with different policies and approaches to content moderation. This ultimately leads to the removal of much arguably inappropriate content without stifling speech outright.

Some may argue that major players like Facebook and Google do not face effective competition. But approaches that attempt to decide uniformly what content should or should not be allowed only serve to entrench these players in their current market position. If one of the major firms begins removing content because they fear losing advertisers, a niche opens. Many users will still want to see that content, and other advertisers will want to reach this audience. Platforms trying to compete can design their moderation policies to target this audience.

Also, opening up platforms to more liability will increase litigation costs for all companies in the marketplace, but the brunt of this weight will be felt by start-up and maverick firms trying

⁵³ 47 U.S.C. § 230(e)(1)-(2).

to compete with the dominant players. This is because the largest firms can already bear the costs of increased litigation and regulation, but smaller firms cannot.⁵⁴ For example, after the GDPR went into effect, Europe saw decreased start-up investment, and the net winners were the large firms who could bear the compliance costs.⁵⁵

But competition doesn't just come from other social media platforms. News-site comments sections, for example, allow users to discuss news stories or share other information. Strong intermediary liability protections allow these sites to utilize these features to allow for more reader engagement and provide a better overall experience. While the approach to attracting users may vary significantly among competing services, these protections apply to almost all players in the online ecosystem, and overbearing regulation could serve to stifle competition and free speech online.

The Internet has enabled innumerable communities to create and share ideas, with image-based memes serving as an innovative way for people to connect and solve problems. Much of that success would not have been possible without protections like Section 230 of the Communications Decency Act. While companies will undoubtedly make mistakes, and bad actors may choose to allow hateful content and disinformation, the continued protection of Section 230 remains essential to ensuring the continued development of online speech in innovative forms such as Internet memes. We know not what the next steps will be in the evolution of online content, but one can be sure it will open new doors for unexpected communities that contribute to the national conversation—doors that future online content policy and platforms shouldn't shut.

⁵⁴ "Section 230 Cost Report," *Engine*, last visited Oct. 7, 2019. https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5c8168cae5e5f04b9a30e84e/1551984843007/Engine_Primer_230cost2019.pdf

⁵⁵ Eline Chivot & Daniel Castro, "The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy," Center for Data Innovation, May 13, 2019. <https://www.datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/>; see also, Eline Chivot & Daniel Castro, "What the Evidence Shows About the Impact of GDPR After One Year," Center for Data Innovation, June 17, 2019. <https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/>; see also, Nick Kostov & Sam Schechner, "GDPR Has Been a Boon for Google and Facebook," *Wall Street Journal*, June 17, 2019. <https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/>.

Mr. Steve Huffman
Page 1

Additional Questions for the Record

**Subcommittee on Communications and Technology and
Subcommittee on Consumer Protection and Commerce
Joint Hearing on
“Fostering a Healthier Internet to Protect Consumers”
October 16, 2019**

Mr. Steve Huffman, Co-Founder & CEO, Reddit, Inc.

The Honorable Anna G. Eshoo (D-CA)

- 1. Just a few years ago, Reddit was involved in many controversies, such as GamerGate, concerning the company’s content moderation practices. Yet you seem to have made changes to your content policies that have, to some degree, cleaned up some of the worst issues. What did you do in the last few years, and how did Section 230 play a role in that process?**

Response: Thank you, Congresswoman, for recognizing this, as it’s something we’ve worked hard at over the past several years and we’re proud of the progress we’ve made, while understanding of course that there is still more work for us to do here. Section 230 has been Reddit’s biggest tool in evolving our content moderation practices. In the past several years we have updated our policies on violent content, on involuntary pornography, on controlled goods, and on bullying and harassment, allowing us to be much more proactive in removing bad material from our site. We’ve also very intentionally grown and built out the teams and tools that we employ to address these problems, and we continue to evolve our approach. It is Section 230 that has allowed us to do all this without either the fear of retribution from bad actors angry that we’ve taken their content down, or of punishment in the form of liability for things that we might miss despite our good-faith efforts.

- 2. Dr. Citron’s idea for including a requirement that platforms employ reasonable content moderation practices to receive Section 230 immunity is an interesting idea. If it was signed into law, how would it affect the business of Reddit?**

Response: The difficulty with Dr. Citron’s new standard is that it turns every content moderation decision our teams make into a court case over whether we were “reasonable” or not in our content moderation practices. Our teams along with our volunteer community moderators have to make very difficult decisions every day. Some people will be upset that their piece of content came down. Others will be upset that another person’s content stayed up. Someone is likely going to be unhappy either way. Dr. Citron’s new standard merely emboldens those unhappy people to go to a trial lawyer and sue us. In order to avail ourselves of Section 230, we would need to prove in court that we have reasonable content moderation practices. I can guarantee you that my definition and your definition of “reasonableness” would be very different from that of a trial lawyer’s.

Mr. Steve Huffman
Page 2

These lawsuits would spell ruin for smaller businesses like ours, while entrenching the largest players in the industry. Even in cases where companies may ultimately prevail in litigation, the legal expenses of defending the case could be existential for startup companies like ours, which are privately-held, still on venture funding, and not yet profitable.

3. **Please tell us about how Reddit responded to the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (Public Law 115–164), better known as FOSTA-SESTA, being signed into law, including its effects, both intended and unintended, and how your company determined how to ensure compliance with the law.**

Response: FOSTA-SESTA has created a chilling effect not only on the Reddit platform but across the internet. Now let us be clear, it is our deeply held belief that content facilitating sex trafficking should never exist on our platform. It is important to note sex trafficking is illegal in the United States, and even before FOSTA-SESTA, Section 230 did not provide immunity regarding this or other criminal activity. What FOSTA-SESTA does do is create a great deal of ambiguity around when a platform has culpable knowledge of trafficking activity. This uncertainty forced Reddit, on the advice of counsel, to take down a number of safety and harm-reduction discussion communities run for, and by, those in the sex work industry, further marginalizing an already at-risk population. And while we understand that some may not consider sex workers to be a particularly sympathetic group, it is not a difficult leap to see the same choices forced around other vulnerable communities that have sparked 230 conversations, such as opiate addiction support and harm reduction communities.

The Honorable Kathy Castor (D-FL)

1. **On June 19, 2019, The Verge published an investigation into one of Facebook’s content moderation sites in Tampa, FL, which is operated by the firm Cognizant. The article details allegations of appalling working conditions including sexual harassment, verbal and physical fights, theft, and general filthiness in addition to adverse mental health effects associated with the nature of their work.**
 - a. **Operationally, how should tech platforms moderate their content? What role should human content moderators play? What role should technology play?**

Response: At Reddit, we’ve found that the only thing that scales with users is users. That is why we’ve empowered each Reddit user to also be a content moderator, and have structured our site in a way that is akin to neighborhoods—manageable units that are familiar to the people in them—so that no one individual or entity needs to have the burden of trying to police the entire site. This structure ensures that our moderation system is sensitive to social and cultural context, since it is community members themselves who voluntarily perform the moderation actions. This type of contextual awareness is something that machines will have a difficult time duplicating.

Mr. Steve Huffman
Page 3

But where machines come in is in giving humans superpowers, and helping humans scale their work. For example, while our in-house content moderators (known as our “Anti-Evil Team”) review Reddit reports individually by hand, those reports are prioritized by machine learning, to help us ensure that the reports that are the most likely to be urgent go to the top of the pile, rather than just being buried chronologically.

Machines can also help cut down on the mundane. For example, we have a tool called “Automoderator,” which is essentially a helper-bot that we have built and made available for Reddit community moderators to use. They can set the Automoderator to do a number of things, such as, for example, banning certain words or slurs from appearing in the community. This is something that is customized from community to community by the volunteer moderators themselves, so that context and nuance is always present. It’s a great example of machines complimenting and amplifying human judgement at scale, reducing the burdens on individuals.

Finally, we also try and reduce the burden on individuals who do this work by always keeping their wellness at front of mind in our policies and practices. We provide them with benefits such as access to counselors, mandatory vacation time, and other measures to fight trauma or burnout. We are also mindful of their needs in the tools we build for them to do their jobs. For example, the interface of the programs that they use to review potentially disturbing content includes features such as progressively blurring, muting, and/or greyscaling images and video where human review is necessary.

b. What standard should a private company use to evaluate content? “Quasi constitutional”, a “community standard” established by the company along the lines of other private media, other?

Response: At Reddit we strongly believe that users themselves need to be empowered in setting appropriate standards. This is why we have created a federal system, wherein we at the corporate level set out topline principles, but beyond that, we empower our individual communities themselves to establish customized rules that are appropriate to their culture and context. We think that such a model is the only thing that scales while being flexible enough to accommodate the vast diversity of people who find their home on Reddit.

c. Given that private companies are not governed by standards that government would be when it decides not to post content, why do content moderators have to spend so much time reviewing and in such great detail evaluating explicit, violent, or hateful content? What value is there to society and the site owner to work to ensure that such explicit, violent, or hateful content is given every opportunity to be posted?

Response: We’d agree that there is little value to a great deal of violent, hateful, or otherwise objectionable content, which is why we are grateful for the way that Section 230 empowers us to exercise judgment to take it down, and take it down quickly. But in our experience, it’s not the obvious, black-and-white cases that take the most time. It’s the grey area content, where different, reasonable, well-intentioned people can disagree on whether something is

Mr. Steve Huffman

Page 4

inappropriate or a violation. That is where we spend the most time. And we think that it is important that we be fair and consistent when these hard cases come up, because that fairness and consistency is what is going to maintain trust with our users, who range the entire political spectrum.

d. This explicit, violent, or hateful content often is known to be inconsistent with the tech platform's content bylaws. Why do tech platforms, like Facebook, force content moderators to not only look at but also evaluate in great detail explicit, violent, or hateful content that is often inconsistent with the tech platform's bylaws?

Response: I can't speak for other companies' practices. But at Reddit, the vast majority (more than 99%) of content moderation is done on a volunteer basis, by users themselves on their own schedule, in their own spaces, and we take their wellbeing seriously. We have an entire team at the company whose job it is to cater to moderator needs and build tools for them. Additionally, as part of our efforts to continually improve the speed and efficacy of our enforcement mechanisms, we are working toward being more proactive around bad content-- that is, taking action on it before a human ever encounters it. For example, like many of our peers, we employ content hashing against child exploitation content and foreign terrorist content, which means that this material comes down swiftly and automatically, without a human having to see it and potentially be traumatized.

e. Should content moderators have more leeway to ban harmful content so they don't have to look at it over such lengthy time periods and evaluate the content in such detail?

Response: Given that more than 99% of content moderation is undertaken on a volunteer basis by users themselves, typically in accordance with rules they themselves have created rather than ones handed down by us, content moderation on Reddit is fundamentally different than the approach other companies take, and has leeway and flexibility inbuilt. For the in-house employee teams that we have that also engage in content moderation, we take their wellbeing enormously seriously. We have in place benefits for them such as mandatory periodic vacation, access to counselors, and other measures to care for them. We also have taken their wellness into account in the tools we build for them to do their jobs. For example, review programs for potentially sensitive or disturbing content includes features such as progressively blurring, muting, and/or gray-scaling images and video where human review is necessary. On top of this, we employ hashing technology around abhorrent illegal content like child exploitation and foreign terrorist propaganda, so that a human never even has to be exposed to it.

f. What should industry best practices be for treating content moderators? Should Congress play a role in ensuring worker rights in this unique industry? If so, how?

Response: There are certain benefits that we give to our employees who handle sensitive content that we believe are a must. This includes mandatory periodic vacation, strictly limited working hours, access to counselors, mental healthcare benefits, and a comfortable, inviting workspace.

Mr. Steve Huffman
Page 5

- g. Is it common practice among tech platforms to use contractors to conduct content moderation for their sites? Why do some tech platforms use contractors to conduct content moderation for their sites? Should tech platforms do this?**

Response: There is actually significant diversity in the industry in how companies approach content moderation, and recognizing that diversity is important. While some of the largest companies use contractors at an industrial scale, that's not really a viable option for smaller companies. We, for example, have chosen to rely on a community moderation model. Other companies do all of their content moderation in-house with small teams. The approach that each company takes largely depends on their individual resources and business model.

The Honorable Lisa Blunt Rochester (D-DE)

- 1. At the October 16, 2019, joint hearing, you provided commitments that Reddit will disclose information on diversity of your content moderators and issues with hiring diverse content moderator teams. Please provide that information to the Energy and Commerce Committee and my office.**

Response: As noted in our annual Transparency Report, over 99% of content moderation actions are done by volunteer moderators, who come from the Reddit userbase itself. Our company has a different business model from others in the industry, in that we don't collect large amounts of user data. In fact, we collect hardly any. This means that we actually know very little about the real-world identities of our users-- we don't know their age, we don't know their gender, we don't know their race, we don't know their religion. However, what we do know is that the moderators of any particular community are invested members of that community, and they are appointed by their peers. This gives us confidence that our moderators are attuned to the special context and needs of the communities that they help govern.

That said, when it comes to our actual employee base, we care deeply about ensuring that we have a broad and diverse team. We track the racial and ethnic makeup of our company, as well as inclusion sentiment amongst our employees, so that we can understand where we are and what further progress we need to make. To help us meet our goals, we recruit from historically black colleges and universities (HBCUs) as well as Hispanic-serving institutions (HSIs), and we sponsor tech events focused on engaging women and minorities. In the past year, these sponsorships have included (among others) AfroTech, /dev/color, Tech Inclusion San Francisco, the Lesbians Who Tech Leadership Summit, and the Grace Hopper Celebration of Women in Computing. We also have employee resource groups for our diverse employees, and tap their opinions on relevant product decisions to ensure that we have diverse viewpoints represented, even if those viewpoints come from different teams than those directly responsible for a particular product or feature.

- 2. What can the federal government do to improve the capacity and ability to effectively moderate online content, including technological research?**

Mr. Steve Huffman
Page 6

Response: The single most important thing the federal government can do is to protect laws like Section 230 that make it possible for us to moderate in good faith without fear of retribution. Aside from that, the federal government should encourage diversity in approaches to online content moderation--whether through academic research into different models of online communities or through encouraging startups that approach content moderation differently from the central model dominant in the social media industry today.

The Honorable Tom O'Halleran (D-AZ)

1. **Mr. Huffman, as written in statute, Section 230 has “good Samaritan” language to incentivize online platforms to take actions “in good faith to restrict access to or the availability of” harmful content.**

Many platforms have established content or use of service policies to specify what behavior is allowed by the service, while others employ artificial intelligence formulas to automatically filter user-generated content. Some platforms also hire human content moderators to review and remove content posted by users on its platforms that is considered harmful, violent, or graphic. These content reviewers often suffer from Post-Traumatic Stress Disorder (PTSD).

- a. **What more can be done by the government and industry to ensure sufficient mental health services are made available to human content reviewers?**

Response: Mental health services are important not only to workers in our industry, but to everyone. But simply recognizing mental health as a priority is a first step. A second step is identifying the breadth of people who come across sensitive content. It's not only the people who directly review content. It's also the people who manage them. Management of sensitive teams is a very important skill, and sensitivity to worker needs is something that needs to permeate an entire organization. For this reason, we offer counseling and mental health benefits directly to the individual employees who undertake such work, and we also train their managers in the special needs that apply to managing such workers.

Additionally, it is important to reduce employee exposure to harmful content in the first place. We try to do this through the tooling we provide teams who fight this content. We have built in safety options that allow reviewers to put the content in grayscale or blur, or mute it by default.

Where government can be helpful in this regard, aside from prioritizing mental healthcare for everyone, is sharing experiences with industry. There are very large numbers of public servants who encounter sensitive or traumatic situations in their work every day, from members of our military to our first responders. These industries have each acquired learnings and tools to help protect the mental wellbeing of their frontline employees. Thinking of content moderators as a

Mr. Steve Huffman
Page 7

type of first responder, and valuing them as such, could go a long way. Encouraging public-private knowledge sharing and best practices in this regard could be extremely productive.

The Honorable Greg Walden (R-OR)

1. **At the hearing, Rep. Bilirakis asked EFF whether they have argued for including language mirroring legislation in trade deals explicitly for the purpose of “baking” language into an agreement to protect the statute domestically.**

For the record, Yes or No: Is including such 230-like language in trade agreements an attempt to preclude us – the committee of jurisdiction – from revisiting the statute?

Response: Respectfully, I’m not qualified to answer that. You’d have to speak to the people who wrote the language.

2. **In your testimony you talk about the importance Reddit places on the downvote feature. Can you describe how this type of moderation applies to the more “edge-cases” of speech issues vs. the clear-cut illegal activity that may find its way on your platform?**

Response: Thank you, Congressman, for making this important distinction. As you’re no doubt aware, there are many things on Reddit, that, while they don’t actually break either the law or our rules, are lower quality and not particularly valuable. In most of these cases, it would be inappropriate overreach for us as a company to take the content down. Not only would it be heavy-handed, it would distract our limited resources from things that are actually dangerous or illegal. Community moderation, and the downvote specifically, is a solution that allows the community itself to say, “we don’t think this content is worthwhile,” and downrank it accordingly, limiting its visibility. Indeed, to think about it in a real-world context, social pressures dictate real-life decorum every day in our lives. Reddit tries to replicate that online.

- a. **Do you think the “user-moderator” approach could be exported to other platforms? If yes, should it? If no, why not?**

Response: There is a wide diversity of site structures and business models in the tech industry, and it’s important to recognize this, and avoid the government dictating any single approach. This is particularly true given the reality of just how fast technology changes. For us and our site structure, at this time, the user-moderator approach has worked well. However, more important than this particular model, which may or may not be right for others in the industry, is the principle from which it draws—that users of a site should be intimately involved in its governance and have a stake in it. This is what makes Reddit different from other sites. We put the user at the center of everything, and actually empower them.

3. **In your testimony, you state that medium, small, and startup-sized companies do not have the resources to moderate content “from the center.” Surely, you’d**

Mr. Steve Huffman
Page 8

agree that some tech companies have the resources to devote to better, more effective moderation. At what point should we consider a company to be big enough to take more responsibility for their platform?

Response: Although smaller companies might not have the resources to moderate content in a centralized way, that doesn't mean that they don't have the resources to moderate content at all. It simply means that they might take a different approach, and we should recognize that and acknowledge that it is healthy for the industry for there to be a diversity of approaches. And to be sure, no matter what the size of a company or which model of content moderation they follow, we can all do better and are continually improving our tools and processes in this regard.

- 4. Some have argued that Section 230 was not intended to provide a liability shield to a nascent industry that needed protection from insurmountable legal fees. See, e.g., Letter from TechFreedom, to U.S. House of Representatives Energy & Commerce Committee, at 11 (dated Oct. 15, 2019). You are in a unique position as head of Reddit to understand the importance of Section 230. Based on your understanding and experience, do you believe Section 230 was designed with companies like Reddit in mind? Should Congress consider the impact any liability carve-outs could have on the ability of smaller platforms to thrive?**

Response: It's hard to look at the case law leading up to 230 and conclude that the drafters didn't have companies like Reddit in mind when they proposed Section 230. If you look at the original Prodigy case that prompted 230, it looks remarkably like Reddit -- a vast system of message boards with good-faith community moderation attempts. Companies were trying to do the right thing, and being punished for it with liability. The incentives were totally backward. If you want a safer internet, you need to ensure that companies are empowered to moderate without fear of liability. On top of that, there are real competition aspects to this question nowadays, particularly when we are talking about costly things such as litigation. Even to bring a case to dismissal costs money in legal fees. Just as an example, some of our competitor companies have more lawyers than we have total employees. They'll survive the onslaught of litigation that even small carve outs to 230 would bring. Companies like Reddit, and those smaller than Reddit, probably wouldn't.

The Honorable Bill Johnson (R-OH)

- 1. How does Reddit distinguish between "unpopular" posts that don't violate your rules from those that do violate the rules?**

Response: There is plenty of content on Reddit, that, while it doesn't break the rules, is unpopular with the community. This is where Reddit's user-based content curation comes in. Any Reddit user may vote on content on Reddit, either up or down. Unpopular content that receives a high amount of downvotes is deprioritized and hidden. All this happens without our direct involvement. It is purely a function of the Reddit community self-governing.

Mr. Steve Huffman
Page 9

2. **You also mentioned in your testimony that you “evolve” your policies “to ensure they keep up with reality.” What kind of updates and how often are you having to make these changes to your policies to keep up with content against your rules and standards?**

Response: Since 2017, we’ve made numerous updates to our sitewide Content Policy. This includes revisions to existing policies, such as our policies against violent content, harassment or bullying, and involuntary pornography. It also includes the creation of entirely new policies, such as a prohibition on the sale of controlled goods. Our policy team is constantly reviewing these rules, including via user feedback, to determine where the gaps are and what else may need to be addressed.

For some specific examples of what this all means, take our most recent update, to our harassment and bullying policy, which we launched this past September. One of the changes that we made, based on feedback from users, was to allow bystanders to report harassment, a departure from our previous practice of accepting reports only from the victims themselves. We thought this was too much of a burden to place on victims, and so we made the change. As another example, we updated our involuntary pornography policy in February 2018 to specifically prohibit faked content. We made the change to address the new problem of pornographic deepfakes, which are nearly always created without the consent of the person depicted.

The Honorable Richard Hudson (R-NC)

1. **One of the best parts of my job is having the privilege of representing the brave men and women who are stationed at Fort Bragg. Additionally, my district represents one of the fastest growing veteran populations in the country. I take it as my responsibility to advocate for them in everything I do. As you all are aware, the opioid epidemic is something that has ravaged our country and disproportionately affected veterans. One of the underlying issues in this area is the availability of these drugs and how easy it can be for an individual to gain access to them. Unfortunately, we have seen that these drugs are often available through illegal online sales that help fuel this crisis.**
 - a. **Can you please explain how your company monitors content on your platform to ensure the illegal sale of opioids does not occur?**

Response: Thank you for the question. Our approach to this content starts with our policies. Last year, we created a new policy explicitly forbidding the use of Reddit for the sale or exchange of controlled goods, which includes prescription opioids and other drugs. The enforcement of this policy is ongoing, and relies on a combination of human monitoring and reporting as well as automated tools. In this regard, we’ve been grateful for the leadership that the FDA has provided on this issue, and we’ve been in touch with them on multiple occasions. Their list of illegal pharmacy warning letters has been an incredibly important resource for us, in terms of providing an authoritative list of unauthorized online pharmacies. We monitor these warning letters, and

Mr. Steve Huffman
Page 10

automatically block the posting of URLs leading to them. Additionally, when we find accounts attempting to post this material, we ban them. We can also apply special technical methods to fight against them from coming back to our site to continue their illegal activity.

On the advertising side, we have a strict advertising policy that has special rules governing the advertising of prescription drugs. All of these advertisements must be pre-approved by our policy team in house, and they must follow all FDA and industry guidelines, including practices such as side-effect labeling. We also prohibit the targeting of prescription drug advertisements to so-called sensitive communities, including communities for addiction recovery, or support communities for those with chronic conditions.

All that said, because of the high monetary stakes involved in the illegal drug trade, this is an ongoing battle, and we are working against a creative and adaptive adversary. These bad actors often use coded or obscure language to make their activity more difficult to detect. Nevertheless, we're committed to continuing our fight against them, while also ensuring that our approach is sensitive and thoughtful enough so as not to wrongly ensnare the many, many users who find support and community on Reddit for their recovery and harm reduction purposes.

b. When you find such content on your platform, do you engage law enforcement in addition to removing the content from your platform?

Response: We cooperate with federal, state, and local law enforcement, as outlined in our Guidelines for Law Enforcement, available publicly on our website. In serious cases of content involving real-world harm, we have made proactive reports to the Northern California Regional Intelligence Center (NCRIC). The NCRIC has proven to be an invaluable resource for escalating issues to law enforcement, especially given the complexity of the different law enforcement agencies that could be involved in an investigation regarding online activity. We hope that Congress, as it makes choices regarding resourcing, continues to support efforts like the NCRIC to better coordinate law enforcement reporting with adequate resources.

Ms. Danielle Keats Citron
Page 1

Additional Questions for the Record

**Subcommittee on Communications and Technology and
Subcommittee on Consumer Protection and Commerce
Joint Hearing on
“Fostering a Healthier Internet to Protect Consumers”
October 16, 2019**

Ms. Danielle Keats Citron, Professor of Law, Boston University School of Law

The Honorable Anna G. Eshoo (D-CA)

- 1. Your idea for including a reasonableness standard in Section 230 is an interesting idea. There are, of course, fringe platforms that have less than reasonable business practices. On the whole, are major tech companies’ current practices reasonable? Is there any entity, regulatory or otherwise, you think could define reasonable in this context, or should courts define it over time?**

Response: Under my proposal with Ben Wittes, platforms would enjoy immunity from liability *if* they could show that their content-moderation practices writ large are reasonable. Our revision to Section 230(c)(1) would read as follows:

No provider or user of an interactive computer service that takes reasonable steps to address unlawful uses of its service that clearly create serious harm to others shall be treated as the publisher or speaker of any information provided by another information content provider in any action arising out of the publication of content provided by that information content provider.

If adopted, the question before the courts in a motion to dismiss on Section 230 grounds would be whether a defendant employed reasonable content moderation practices in the face of unlawful activity. The question would *not* be whether a platform acted reasonably with regard to a specific use of the service. Instead, the court would ask whether the provider or user of a service engaged in reasonable content moderation practices writ large with regard to unlawful uses that clearly create serious harm to others.

The reasonableness of a company’s content moderation practices depends upon the practices and content in question. Courts are well suited to address the reasonableness of a platform’s speech policies and practices vis-à-vis particular forms of illegality that cause clear harm to others (at the heart of a litigant’s claims), as my proposal with Benjamin Wittes (hereinafter “Proposal”) suggests. Reasonableness is an effective tool because it will evolve as best practices and technologies do. What is reasonable policy vis-à-vis involuntary pornography today may be different over time, especially as technologies change.

Ms. Danielle Keats Citron

Page 2

Reasonableness does not anticipate a one-size-fits-all approach but rather is tailored to the problem at hand and the size and nature of the work of the platform. Today, Facebook's policy on nonconsensual porn exemplifies reasonable approach given the scale of the problem and the harm at issue. Indeed, with its hashing program, Facebook is operating at the cutting edge of best practices. As technology and practices develop, Facebook's policies and practices may need to evolve as more effective tools and strategies to address nonconsensual pornography become available.

The Honorable Kathy Castor (D-FL)

1. **On June 19, 2019, The Verge published an investigation into one of Facebook's content moderation sites in Tampa, FL, which is operated by the firm Cognizant. The article details allegations of appalling working conditions including sexual harassment, verbal and physical fights, theft, and general filthiness in addition to adverse mental health effects associated with the nature of their work.**

- a. **Operationally, how should tech platforms moderate their content? What role should human content moderators play? What role should technology play?**

Response: Best practices for content moderation—speech policies and practices—depend upon the issue at hand and the platform in question. Some issues require human judgment. This is true of threats. “I want to kill you” could be an affectionate rib between friends or a genuine terroristic threat. Context is key. Algorithms could flag content for a reviewer but in the end the contextual inquiry must be made by a human being.

Let's consider an example. For child sexual exploitation (CSE) material and child pornography, companies rely on algorithmic flagging to filter and block content in connection with NCMEC's database of hashed images flagged as CSE material. Human reviewers may see CSE material that is not already in the NCMEC database but a considerable amount is dealt with via an automated filtering system.

- b. **What standard should a private company use to evaluate content? “Quasi constitutional”, a “community standard” established by the company along the lines of other private media, other?**

Response: The standard of reasonableness would derive from the liability at issue. To start, Plaintiffs need a theory of relief to bring against a site. Content platforms are not strictly liable for content on their sites. A plaintiff, for instance, could bring potential claims like defamation (as publisher or distributor) or negligent enablement of crime against a site. Then, the question is whether the platform responded reasonably to types of unlawful activity alleged—defamation or negligent enablement of crime—causing clear harm to others.

Ms. Danielle Keats Citron

Page 3

Suppose victims of nonconsensual pornography sue a social network for negligent enablement of the crime of invasion of sexual privacy. Plaintiffs allege that the site has a clear policy banning nonconsensual posting of intimate images but has done nothing to respond to their complaints. The site moves to dismiss the suit on Section 230 grounds alleging that it has responded reasonably to nonconsensual pornography (NCP) complaints. Suppose further that the site employs 50 content moderators who regularly respond to complaints about NCP within a week's time. The site has a user-friendly process to report abuse. The court may grant the defendant's motion to dismiss on Section 230 grounds, reasoning that the site has a reasonable process to deal with NCP even though the site's moderators failed to respond responsibly in Plaintiffs' case. The key is the reasonableness of the site's NCP practices writ large, not its response in any given case.

If Section 230 were amended along the lines that Ben Wittes and I have suggested, a legal shield would apply to sites sued as publishers or speakers that *takes reasonable steps to address unlawful uses of its service that clearly create serious harm to others*. The reasonableness question only addresses a site's response to (1) unlawful uses of its services that (2) clearly create serious harm to others. The immunity would only come into play if we were talking about proscribable illegality that causes clear harm to others. Generally speaking, the First Amendment protects hate speech and violent imagery. There, the immunity has no application because there would be no basis to sue that would be consistent with the First Amendment.

- c. Given that private companies are not governed by standards that government would be when it decides not to post content, why do content moderators have to spend so much time reviewing and in such great detail evaluating explicit, violent, or hateful content? What value is there to society and the site owner to work to ensure that such explicit, violent, or hateful content is given every opportunity to be posted?**

Response: You are absolutely right. Sites have the freedom to remove content that law cannot prohibit like pornography and hate speech. No doubt, private companies would argue that those decisions reflect their self-expression. They would argue that they are First Amendment rights holders and thus can make any choice they wish about what content appears on their platforms.

Some companies do spend time and money addressing hate speech. They have speech rules and policies banning legally protected speech. Sometimes, their terms of service bans stem from pressure coming from EU lawmakers and law enforcers, as I have written about in the Notre Dame Law Review. Sometimes, advocates and advertisers convince sites to remove hate speech because users do not like it. Sometimes, platforms think it is not good for business to host pornography (Facebook is a case in point) even though porn is legally protected speech.

The problem is that there are still many other sites that do host illegality because it attracts eyeballs and thus ad revenue. Sites host nonconsensual pornography, threats, and deep fake sex videos because it is salacious and earns ad revenue. Those sites do not deserve Section 230 immunity.

Ms. Danielle Keats Citron

Page 4

- d. This explicit, violent, or hateful content often is known to be inconsistent with the tech platform's content bylaws. Why do tech platforms, like Facebook, force content moderators to not only look at but also evaluate in great detail explicit, violent, or hateful content that is often inconsistent with the tech platform's bylaws?**

Response: Why do they have speech policies that effectuate their rules? Like a diner that says customers have to wear shirts, a site may have rules banning hate speech. The incentives for having and enforcing such rules are outlined in my answer to (c).

- e. Should content moderators have more leeway to ban harmful content so they don't have to look at it over such lengthy time periods and evaluate the content in such detail?**

Response: I imagine that is covered by the terms of their contract with their employers.

- f. What should industry best practices be for treating content moderators? Should Congress play a role in ensuring worker rights in this unique industry? If so, how?**

Response: The same rules apply to workplaces of content moderators as other firms of their size in the United States. Title VII would address workplace sexual harassment so long as firms had 50 employees. It may become apparent to Congress that new workplace safety rules are needed to address smaller firms including content moderators.

- g. Is it common practice among tech platforms to use contractors to conduct content moderation for their sites? Why do some tech platforms use contractors to conduct content moderation for their sites? Should tech platforms do this?**

Response: Yes, see Sarah Roberts's important new book called *Behind the Screen* on this point. They likely use contractors because it is cheaper. If Congress thinks that such practices undermine worker rights then I hope Congress addresses this inequity.

The Honorable Lisa Blunt Rochester (D-DE)

- 1. What can the federal government do to improve the capacity and ability to effectively moderate online content, including technological research?**

Response: I do not imagine a role for the federal government in the content moderation process. My strong inclination is to keep the incentives where they are—on encouraging private companies to moderate their own platforms and using the legal shield of Section 230 as that incentive but conditioning the incentive on responsible (reasonable) practices.

Ms. Danielle Keats Citron

Page 5

The Honorable Greg Walden (R-OR)

1. **How do app stores differ from social media sites with regard to their responsibilities to moderate content?**

Response: App stores may have different responsibilities than content platforms like social networks. The answer would depend on the allegedly wrongful behavior of the app store and the liability alleged.

2. **It's clear from the Congressional record that the authors of Section 230 recognized the need for industry to take responsibility to moderate their platforms because no government bureaucracy could regulate the vast content on the Internet. In Dr. Farid's testimony, he cites "fear" as the reason for inaction since PhotoDNA has been widely deployed and successful; that the success of PhotoDNA would show CSAM could be removed and quote, "the technology sector would have no defense for not contending with myriad abuses on their services."**

What is it that has failed to encourage more research and deployment of similar technologies to address other illegal activity? Market forces? Fear?

Response: There is no legal shield against federal criminal law. Hence, site operators can be held liable for publishing child porn. As a result, sites have a strong incentive to cooperate with NCMEC and filter child porn. There, incentives are operating well. For tortious user activity, however, sites have no such incentive. Section 230(c)(1) provides a legal shield for under filtering without the condition of responsible or reasonable content moderation practices. Thus, we need law to provide that incentive.

3. **In an October 15, 2019 letter to the Energy & Commerce Committee (herein after "Letter"), TechFreedom conclusively states that there is no implicit quid pro quo embodied in Section 230, granting Internet platforms liability protections in return for keeping offensive and violent content off their platforms. See, e.g., Letter from TechFreedom, to U.S. House of Representatives Energy & Commerce Committee, at 1-2 (dated Oct. 15, 2019). Has this quid pro quo, however, been recognized by federal courts? See, e.g., Blumenthal v. Drudge, 992 F.Supp. 44, 52 (D.D.C. 1998) ("In some sort of tacit quid pro quo arrangement with the service provider community, Congress has conferred immunity from tort liability as an incentive to Internet service providers to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted.")**
 - a. **In this letter, the author states that, "The Republican Staff Memo claims that Section 230 has been interpreted more broadly than Congress intended: 'While the authors intended this liability protection to incentivize 'interactive computer services' to patrol their platforms, it was not intended to be interpreted as an unlimited, broad liability**

Ms. Danielle Keats Citron
Page 6

protection absent any good faith action to maintain accountability.” See, Letter, at 5.

Response: The lower federal courts and state courts have *not* found that Section 230(c)(1) is conditional on responsible practices, as the drafters intended. That is why Ben Wittes and I argue that Section 230(c)(1) should be made conditional (see language above) explicitly.

b. Have the courts interpreted Section 230 more broadly than Congress intended? If so, which cases highlight such a diversion?

Response: Courts have stretched Section 230 far beyond what its words, context, and purpose support.¹ Section 230 has been read to immunize platforms from liability that:

- knew about users’ illegal activity, deliberately refused to remove it, and ensured that those responsible could not be identified;²
- solicited users to engage in tortious and illegal activity;³ and
- designed their sites to enhance the visibility of illegal activity and to ensure that the perpetrators could not be identified and caught.⁴

Courts have attributed this broad-sweeping approach to the fact that “First Amendment values [drove] the CDA.”⁵ For support, courts have pointed to Section 230’s “findings” and “policy” sections, which highlight the importance of the “vibrant and competitive free market that presently exists” for the internet and the internet’s role in facilitating “myriad avenues for intellectual activity” and the “diversity of political discourse.”⁶ As Mary Anne Franks has underscored, Congress’ stated goals also included the:

development of technologies that “maximize user control over what information is received” by Internet users, as well as the “vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking and harassment by means of the computer.” In other words, the law [wa]s intended to promote the values of privacy, security and liberty alongside the values of open discourse.⁷

Section 230’s liability shield has been extended to activity that has little to do with free speech, such as the sale of dangerous products.⁸ Consider Armslist.com, the self-described “firearms marketplace.”⁹ Unlicensed gun sellers use the site to find buyers who cannot pass background

¹ Citron & Wittes, *supra* note, at 406-10.

² *Id.*

³ *Id.*

⁴ Citron, *Section 230’s Challenge to Civil Rights and Civil Liberties*. See generally Olivier Sylvain, *Intermediary Design Duties*, 50 CONN. L. REV. 1 (2017).

⁵ *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 18 (1st Cir. 2016), cert. denied, 137 S. Ct. 622 (2017).

⁶ See, e.g., *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009).

⁷ Mary Anne Franks, *The Lawless Internet? Myths and Misconceptions About CDA Section 230*, HUFFINGTON POST (Feb. 17, 2014).

⁸ See, e.g., *Hinton v. Amazon.com, LLC*, 72 F. Supp. 3d 685, 687, 690 (S.D. Miss. 2014).

⁹ <https://www.armslist.com/>

Ms. Danielle Keats Citron

Page 7

checks.¹⁰ Armslist.com is where Radcliffe Haughton illegally purchased a gun.¹¹ Haughton's estranged wife obtained a restraining order against him that banned him from legally purchasing a firearm.¹² On Armslist.com, Haughton found a gun seller that did not require a background check and purchased a gun.¹³ He used that gun to murder his estranged wife and her two co-workers.¹⁴ The Wisconsin Supreme Court found Armslist immune from liability based on Section 230.¹⁵

Extending Section 230's shield from liability to platforms that deliberately encourage, facilitate, or refuse to remove illegal activity would seem absurd to the CDA's drafters. But even more absurd to them would be immunizing from liability enterprises that have nothing to do with moderating online content, such as marketplaces that connect sellers of deadly weapons with prohibited buyers for a cut of the profits. Armslist.com can hardly be said to "provide 'educational and informational resources' or contribute to 'the diversity of political discourse.'"¹⁶

4. Can you please explain why you believe market forces will likely not encourage more responsible content moderation but may actually produce the opposite?

Response: Market forces alone are unlikely to encourage responsible content moderation. Platforms make their money through online advertising generated when users like, click, and share.¹⁷ Allowing attention-grabbing abuse to remain online accords with platforms' rational self-interest.¹⁸ Platforms "produce nothing and sell nothing except advertisements and information about users, and conflict among those users may be good for business."¹⁹ If a company's analytics suggest that people pay more attention to content that makes them sad or angry, then the company will highlight such content.²⁰ Research shows that people are more attracted to negative and novel information.²¹ Thus, keeping up destructive content may make the most sense for a company's bottom line.

As Federal Trade Commissioner Rohit Chopra powerfully warned in his dissent from the agency's 2019 settlement with Facebook, the behavioral advertising business model is the "root cause of [social media companies'] widespread and systemic problems."²² Online behavioral advertising generates profits by "turning users into products, their activity into

¹⁰ See Mary Anne Franks, *Our Collective Responsibility for Mass Shootings*, N.Y. TIMES, October 11, 2019, available at <https://www.nytimes.com/2019/10/09/opinion/mass-shooting-responsibility.html>.

¹¹ *Id.*

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.* The non-profit organization the Cyber Civil Rights Initiative, of which one of us (Franks) is the President and one of us (Citron) is the Vice President, filed an amicus brief in support of the petitioner's request for writ of certiorari in the Supreme Court. Brief of Amicus Curiae of Cyber Civil Rights Initiative and Legal Academics in Support of Petitioners in Yasmine Daniel v. Armslist.com, available at https://www.supremecourt.gov/DocketPDF/19/19-153/114340/20190830155050530_Brief.PDF.

¹⁶ Amicus Curiae of Cyber Civil Right Initiative, *supra* note, at 16.

¹⁷ Mary Anne Franks, *Justice Beyond Dispute*, 131 HARV. L. REV. 1374, 1386 (2018) (reviewing ETHAN KATSH & ORNA RABINOVICH-EINY, *DIGITAL JUSTICE: TECHNOLOGY AND THE INTERNET OF DISPUTES* (2017)).

¹⁸ Danielle Keats Citron, *Cyber Mobs, Disinformation, and Death Videos: The Internet As It Is (and as It Should Be)*, 118 MICH. L. REV. (forthcoming 2020).

¹⁹ *Id.*

²⁰ Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.*, Commission File No. 1823109, at 2 (July 24, 2019).

²¹ *Id.*

²² *Id.*

Ms. Danielle Keats Citron

Page 8

assets,” and their platforms into “weapons of mass manipulation.”²³ Tech companies “have few incentives to stop [online abuse], and in some cases are incentivized to ignore or aggravate [it].”²⁴

To be sure, the dominant tech companies have moderated certain content by shadow banning, filtering, or blocking it.²⁵ They have acceded to pressure from the European Commission to remove hate speech and terrorist activity.²⁶ They have banned certain forms of online abuse, such as nonconsensual pornography and threats, in response to pressure from users, advocacy groups, and advertisers.²⁷ They have expended resources to stem abuse that threatened their bottom line.²⁸

Yet market pressures do not always point in that direction. The business model of some sites is abuse because it generates online traffic, clicks, and shares.²⁹ Thanks to online advertising revenue, deepfake pornography sites³⁰ as well as revenge porn sites and gossip sites³¹ are thriving.

The Honorable Michael Burgess (R-TX)

- 1. Mrs. Citron, section 230 of the Communications Decency Act provides liability protections for interactive computer services if they take steps to moderate harmful and illegal content. As a result, Internet platforms have created terms of service for content that they believe reflect the public interest. While harmful content can be identified by algorithms or artificial intelligence, humans are often the final decision-maker in removal of content.**

- a. How can we better incentivize fair and accurate content moderation by Internet platforms that have Section 230 liability protections?**

²³ *Id.*

²⁴ Franks, *Justice Beyond Dispute*, *supra* note, at 1386.

²⁵ Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035 (2018); Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for the Information Age*, 91 B.U. L. REV. 1435, 1468-71 (2011).

²⁶ Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, *supra* note, at 1038-39.

²⁷ *Id.* at 1037.

²⁸ CITRON, HATE CRIMES IN CYBERSPACE, *supra* note, at 229 (discussing how Facebook changed its position on pro rape pages after fifteen companies threatened to pull their ads); Mary Anne Franks, “Revenge Porn” Reform: A View from the Front Lines, 69 FLA. L. REV. 1251 (2017).

²⁹ For instance, eight of the top ten pornography websites host deepfake pornography, and there are nine deepfake pornography websites hosting 13,254 fake porn videos (mostly featuring female celebrities without their consent). These sites generate income from advertising. Indeed, as the first comprehensive study of deepfake video and audio explains, “deepfake pornography represents a growing business opportunity, with all of these websites featuring some form of advertising.” Deeptrace Labs, *The State of Deepfakes: Landscape, Threats, and Impact* 6 (September 2019), available at <https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf>.

³⁰ *Id.*

³¹ See, e.g., *Erna Besic Psycho Mom of Two!*, THE DIRTY (Oct. 9, 2019, 10:02 AM), <https://thedirty.com/#post-2374229>.

Ms. Danielle Keats Citron

Page 9

Response: My proposal with Ben Wittes is designed to provide an incentive to content platforms to engage in responsible content moderation practices where no such legal incentive exists today. Today, under Section 230(c)(1), a content platform enjoys the legal shield for hosting user content even though the platform acted irresponsibly. Our proposal would keep the immunity but explicitly condition it on reasonable content moderation practices as discussed below.

Under our proposal, platforms would enjoy immunity from liability *if* they could show that their content-moderation practices writ large are reasonable. The revision to Section 230(c)(1) would read as follows:

No provider or user of an interactive computer service that *takes reasonable steps to address unlawful uses of its service that clearly create serious harm to others* shall be treated as the publisher or speaker of any information provided by another information content provider *in any action arising out of the publication of content provided by that information content provider.*

If adopted, the question before the courts in a motion to dismiss on Section 230 grounds would be whether a defendant employed reasonable content moderation practices in the face of unlawful activity. The question would *not* be whether a platform acted reasonably with regard to a specific use of the service. Instead, the court would ask whether the provider or user of a service engaged in reasonable content moderation practices writ large with regard to unlawful uses that clearly create serious harm to others.³²

The assessment of reasonable content-moderation practices would take into account differences among online entities. Social networks with millions of postings a day cannot plausibly respond to complaints of abuse immediately, let alone within a day or two. On the other hand, they may be able to deploy technologies to detect and filter content that they previously determined was unlawful.³³

The duty of care will evolve as technology improves and as new threats emerge. There is no one size fits all approach to responsible content moderation. Unlawful activity changes and morphs quickly online and the strategies for addressing unlawful activity clearly causing serious harm should change as well. A reasonableness standard would adapt and evolve to address those changes.

A reasonable standard of care will reduce opportunities for abuse without interfering with the further development of a vibrant internet or unintentionally turning innocent platforms into involuntary insurers for those injured through their sites. Approaching the problem as one of

³² Tech companies have signaled their support as well. For instance, IBM issued a statement saying that Congress should adopt the proposal and wrote a tweet to that effect as well. Ryan Hagemann, *A Precision Approach to Stopping Illegal Online Activities*, IBM THINK POLICY (July 10, 2019), <https://www.ibm.com/blogs/policy/cda-230/>; see also @RyanLeeHagemann, TWITTER (July 10, 2019, 3:14 PM), <https://twitter.com/RyanLeeHagemann/status/1149035886945939457?s=20> (“A special shoutout to @daniellecitron and @benjaminwittes, who helped to clarify what a moderate, compromise-oriented approach to the #Section230 debate looks like.”).

³³ Citron, *Sexual Privacy*, *supra* note (discussing Facebook’s hashing initiative to address nonconsensual distribution of intimate images).

Ms. Danielle Keats Citron
Page 10

setting an appropriate standard of care more readily allows differentiating between different kinds of online actors. Websites that solicit illegality or that refuse to address unlawful activity that clearly creates serious harm should not enjoy immunity from liability. On the other hand, social networks that have safety and speech policies that are transparent and reasonably executed at scale should enjoy the immunity from liability as the drafters of Section 230 intended.

Law should change to ensure that such power is wielded responsibly. With Section 230, Congress sought to provide incentives for “Good Samaritans” engaged in efforts to moderate content. Their goal was laudable. Section 230 should be amended to condition the immunity on reasonable moderation practices rather than the free pass that exists today. Market pressures and morals are not always enough, and they should not have to be.

b. How can we make terms of service more understandable for the average consumer so that they know what content is acceptable and when to identify user content as harmful?

Response: Congress could condition Section 230 on reasonable content moderation practices that include both transparency (clear speech rules and policies) and accountability (giving users a reason for their decisions as to complaints about their content and a chance to respond). My book *Hate Crimes in Cyberspace* calls this a form of technological due process.

2. Mrs. Citron, since the 1990s the Internet has flourished, providing opportunities for business development and free expression. However, some individuals have used the Internet to engage in activity that, if conducted offline, would be illegal. For example, the illegal sale of firearms, prescription of illicit drugs, and the facilitation of human trafficking. Congress recently removed liability protections for Internet platforms that hosted sex trafficking content.

a. How do Section 230 liability protections apply to other content that would be illegal if conducted offline?

Response: Section 230, as it currently is interpreted, has shielded platforms from liability in cases where they would be liable if the activity occurred offline. Take the Armslist case. There, the site got a cut of illegal gun sales. If the site ran a store and allowed parties to come into the store to sell guns without background checks, then the site might be liable under state law. Yet because the site enabled the illegal gun sale online, the legal shield prevented the litigation.

3. Despite the cover of Section 230 liability protections, many Internet platforms do not effectively moderate illegal activity or content.

a. What obstacles prevent Internet platforms from moderating, and removing, explicitly illegal content?

Response: Section 230 actually incentivizes rather than impedes the removal of content, conditioning it on good faith.

Ms. Danielle Keats Citron
Page 11

The Honorable Adam Kinzinger (R-IL)

1. **Professor Citron, a common theme in your testimony—as well as the submitted testimonies of Professor Farid and Ms. Peters—was one of “incentives.” Section 230 of the Communications Decency Act was meant to encourage online platforms to rid their platforms of bad behavior in exchange for liability limitations, yet the examples you all point to suggest the platforms are not delivering on that promise.**
 - a. **I'm not sure yet whether we should amend Section 230, but if the platforms want to keep the benefits of Section 230, don't they need to do a better job of demonstrating what they claim—that they are able and willing to curb illegal activity?**

Response: Content platforms do need to do a better job to act like Good Samaritans as the drafters of Section 230 wanted. There are sites devoted to illegality, from deep fake sex videos and revenge porn to illegal gun sales. Those sites should not enjoy the legal shield. They are far from the Good Samaritans imagined by Reps. Cox and Wyden. We need to condition the legal shield on responsible practices.

Dr. Corynne McSherry, Ph.D.
Page 1

Additional Questions for the Record

**Subcommittee on Communications and Technology and
Subcommittee on Consumer Protection and Commerce
Joint Hearing on
“Fostering a Healthier Internet to Protect Consumers”
October 16, 2019**

Dr. Corynne McSherry, Ph.D., Legal Director, Electronic Frontier Foundation

The Honorable Anna G. Eshoo (D-CA)

- 1. Even if we leave Section 230 as it is, how do you think we should deal with the illegal sales of opioids, the rise in child sex abuse imagery, or any other major content issue we see today?**

Response: For content that is illegal under federal criminal law (as the examples provided are), Congress should look to increased enforcement of existing federal criminal law as a first measure. Congress could also provide additional resources for increased law enforcement against direct perpetrators.

For example, a recent study laid out how drug companies wooed physicians and prescribers “with speaking fees, free dinners, paid trips, and more . . . to convince [them], contrary to the evidence, that the narcotics were safe and effective, persuading them to prescribe far more of the drugs.”¹ Studies like this suggest that it would be more effective to target those companies (as is already underway) than looking to social media companies to police content on the Internet.

Congress should be very careful to avoid collateral damage, such as regulations that might encourage platforms to takedown posts and groups aimed at harm reduction.²

a. Should Congress do anything else to incentivize content moderation?

Response: Most, if not all, of the major platforms already do a significant amount of content moderation. And much of it is highly problematic from a human rights perspective, with the speech of those holding minority views frequently being most vulnerable. We respectfully suggest that a better question is how to encourage them to do a better job of it.

Congress should first understand there are significant First Amendment issues that will arise with any content-based restriction on speech or compulsion to speak. Congress should also understand

¹ German Lopez, *We now have more proof that drug companies helped cause the opioid epidemic*, Vox (Jan. 25, 2019) <https://www.vox.com/future-perfect/2019/1/25/18188542/opioid-epidemic-marketing-overdose-death-purdue>.

² Maia Szalavitz, *Facebook Is Censoring Posts That Could Save Opioid Users’ Lives*, Vice (Jul. 2, 2019) https://www.vice.com/en_us/article/qv75ap/facebook-is-censoring-harm-reduction-posts-that-could-save-opioid-users-lives.

Dr. Corynne McSherry, Ph.D.

Page 2

that it is practically impossible for anyone operating at scale to moderate content perfectly, or even well. Content moderation is a fundamentally thorny activity, prone to subjective choices, cultural clashes, robot flaws, and disparities in reporting patterns that can disproportionately affect specific people and vulnerable communities.³ Platforms should align their policies with human rights norms and apply those policies consistently. At the same time, different platforms should be able to take different moderation choices, indeed, we should value and foster a panoply of platforms with difference features and methods of organizing and displaying content. However, platforms should make their moderation choices and policies explicit.

Accordingly, our own strategy has been to urge platforms to adopt robust transparency and due process measures. That is why we joined other organizations in devising and spurring a set of principles on platforms' transparency, due process, and accountability in content moderation.⁴ Having precise information on how they carry out their moderation activities (both the policies themselves and how they are enforced) and ensuring due process through meaningful notice and appeal mechanisms are essential to making platforms' policies and practices more consistent with human rights law. Greater algorithmic transparency through independent audits would also be valuable.

b. Should Congress update our federal criminal statutes?

Response: If Congress believes that there is an unprotected category of speech under the First Amendment that is not currently covered by federal criminal law, it could pursue that strategy. But any law criminalizing protected expression because of its content will need to satisfy First Amendment strict scrutiny independent of Section 230.

2. Platforms have been criticized for doing too much moderation (particularly with respect to political biases) as well as doing too little moderation (particularly with respect to streaming of mass shootings). Which criticism, if any, is more accurate?

Response: Both and neither. While we certainly agree that online platforms have created content moderation systems that remove speech, we don't see evidence of systemic partisan bias. What we do see are content removal practices that seem to be inconsistent, arbitrary, and non-transparent. We are also concerned that content moderation is too often under pressure from powerful actors, be those non-democratic governments or those with significant economic leverage.

That said, the question points to a concern we share: the need for more empirical data, particularly from the platforms themselves. We know that platforms erroneously remove considerable amounts of content that does not violate their rules, but we have little data on

³ Jillian C. York and Corynne McSherry, *Content Moderation is Broken. Let Us Count the Ways*, Electronic Frontier Foundation (29 April 2019). Available at <https://www.eff.org/pt-br/deeplinks/2019/04/content-moderation-broken-let-us-count-ways>

⁴ Santa Clara Principles, <https://santaclaraprinciples.org>

Dr. Corynne McSherry, Ph.D.

Page 3

precisely how much. Of the major social media platforms, only one company, Reddit, provides data on the number of appeals received and their aggregate outcomes.^{5,6}

The Honorable Kathy Castor (D-FL)

1. **On June 19, 2019, The Verge published an investigation into one of Facebook’s content moderation sites in Tampa, FL, which is operated by the firm Cognizant. The article details allegations of appalling working conditions including sexual harassment, verbal and physical fights, theft, and general filthiness in addition to adverse mental health effects associated with the nature of their work.**
 - a. **Operationally, how should tech platforms moderate their content? What role should human content moderators play? What role should technology play?**

Response: The labor conditions of content moderation are a serious problem. Prof. Sarah T. Roberts at UCLA has done extensive research and writing on this topic and we highly recommend her work.⁷

But content moderation that relies entirely on technology is not the solution either. Filtering mechanisms can be useful in *flagging* material that might violate a platform’s policies, but they cannot substitute for human judgment. Content decisions are almost always deeply contextual in ways that technology cannot discern, and technological screening without human review inevitably leads to over-moderation. This is one of the impossible problems with content moderation, and policy decisions must be made knowing that it is unsolvable.

One useful approach, however, is to put more power in the hands of users themselves to determine what they do and do not want to see. Rather than calling on the platforms to police online speech via an army of underpaid workers, we could call on them to help users control their own social media experience.

- b. **What standard should a private company use to evaluate content? “Quasi constitutional”, a “community standard” established by the company along the lines of other private media, other?**

Response: Each platform has a First Amendment right to decide what content it wants to host, and users are best served by having a variety of options available to them. Some users may prefer a site with minimal moderation. Some might prefer a site limited to specific subject matters or

⁵ Gennie Gebhart, *Who Has Your Back? Censorship Edition 2019*, Electronic Frontier Foundation (June 12, 2019) <https://www.eff.org/wp/who-has-your-back-2019#reddit>

⁶ Reddit Transparency Report 2018, <https://www.redditinc.com/policies/transparency-report-2018>

⁷ Sarah T. Roberts, *Behind the Screen, Content Moderation in the Shadows of Social Media*, Yale University Press (<https://yalebooks.yale.edu/book/9780300235883/behind-screen>)

Dr. Corynne McSherry, Ph.D.

Page 4

communities. Some may want a site that comports with their own standards; some may seek to learn about others' values and perspectives. Quasi-legal standards are difficult given that legal protections vary internationally and almost all platforms serve users around the world.

Rather than dictate specific content policies, we urge platforms to clearly indicate to their users what their standards are, to apply those standards as consistently as possible, to notify users when content (their own and others') has been removed, to provide avenues of appeal of moderation decisions, and to allow outside access to their decision-making so that it can be independently assessed.

- c. Given that private companies are not governed by standards that government would be when it decides not to post content, why do content moderators have to spend so much time reviewing and in such great detail evaluating explicit, violent, or hateful content? What value is there to society and the site owner to work to ensure that such explicit, violent, or hateful content is given every opportunity to be posted?**

Response: As noted, moderators, and the platforms that hire them, face an intractable problem: huge swathes of online content simply doesn't fit into a pre-specified, universally understood category. What one user considers hateful another may consider valuable social commentary. What one user considers sexually explicit, another may consider artistic. Of course, some decisions may be easier than others, but many are not.

With female nudity, for example, moderators seem to struggle to differentiate between with artistic, breast-feeding, and sexualized images. And while much violent content may serve little purpose, other violent imagery, such as that emerging from Syria, may be used to build an important historical record.

- d. This explicit, violent, or hateful content often is known to be inconsistent with the tech platform's content bylaws. Why do tech platforms, like Facebook, force content moderators to not only look at but also evaluate in great detail explicit, violent, or hateful content that is often inconsistent with the tech platform's bylaws?**

Response: We can't speak for all platforms. But from a human rights perspective, content should not be removed from a platform unless an informed decision has been made that removal is appropriate. Because those decisions are frequently not obvious and highly contextual, there must be a human in the loop.

- e. Should content moderators have more leeway to ban harmful content so they don't have to look at it over such lengthy time periods and evaluate the content in such detail?**

Response: We're concerned that such shortcuts will lead to the over-removal of content. As previously noted, moderators already make a significant number of errors.

Dr. Corynne McSherry, Ph.D.
Page 5

- f. What should industry best practices be for treating content moderators? Should Congress play a role in ensuring worker rights in this unique industry? If so, how?**

Response: We are not worker rights experts, but it is clear from recent reports that this is a very challenging issue. We urge Congress to commission further factfinding in this area.

- g. Is it common practice among tech platforms to use contractors to conduct content moderation for their sites? Why do some tech platforms use contractors to conduct content moderation for their sites? Should tech platforms do this?**

Response: These are excellent questions, but workforce policy questions are outside of EFF's expertise.

The Honorable Lisa Blunt Rochester (D-DE)

- 1. What can the federal government do to improve the capacity and ability to effectively moderate online content, including technological research?**

Response: At a minimum, the government could fund research into tools that give users more power over their Internet experience. In addition, Congress should review and reform legal impediments to add-on innovation so that the private sector can offer the same kinds of tools. This includes reforming laws that are doing little to accomplish their intended purpose, and instead being misused to hinder innovation, such as the Computer Fraud and Abuse Act,⁸ and Section 1201 of the Digital Millennium Copyright Act.⁹

The Honorable Tom O'Halleran (D-AZ)

- 1. Dr. McSherry, in your testimony you state how changes to Section 230 could increase liability risks for platforms and force some to over-censor due to a lack of resources to review content as a result. Craigslist's decision to remove its personal ads section is the example you used.**
- a. With the increasing amount of user-generated content being published on platforms daily, what do you believe to be the correct balance between using algorithms and human reviewers for platforms moderating content?**

⁸ *Computer Fraud And Abuse Act Reform*, Electronic Frontier Foundation <https://www.eff.org/issues/cfaa>

⁹ House Committee on the Judiciary Subcommittee on Courts, Intellectual Property and the Internet, Hearing: "Chapter 12 of Title 17", Testimony of Corynne McSherry, September 17, 2014, <https://www.eff.org/files/2014/09/17/09.17.14-testimony-eff.pdf>

Dr. Corynne McSherry, Ph.D.

Page 6

Response: There is no one-size-fits-all approach. The correct balance will likely depend on the particular platform and may vary according to particular categories of content. Algorithmic technology may work for preliminary identifying, sorting, and flagging of some types of visual content, but content flagged by algorithms must still be reviewed by humans to ensure that content is not wrongfully removed. Furthermore, given the nuance required for adjudicating text-based content, that task is best left to human moderators.

The Honorable Greg Walden (R-OR)

1. **At the hearing, Rep. Bilirakis asked you whether EFF has argued for including language mirroring legislation in trade deals explicitly for the purpose of “baking” language into an agreement to protect the statute domestically.**

For the record, Yes or No: Is including 230-like language in trade agreements an attempt to preclude us – the committee of jurisdiction – from revisiting the statute?

Response: No. Including Section 230-like language in a trade agreement may reflect international support for its core principles and could facilitate Internet commerce and expression. But the existence of such language would not prevent this committee from revisiting the statute.

In general, however, trade agreements are not the best vehicle for addressing questions involving fundamental rights such as free expression and access to information. The article to which Mr. Bilirakis referred expressed this very concern.

If Congress wants to ensure that the rights of Internet users are heard in trade agreements, it should seek to fundamentally reform the process by which trade agreements are developed, to ensure much greater transparency and accountability.

The Honorable Adam Kinzinger (R-IL)

1. **Dr. McSherry, you state in your testimony that “victims can use defamation, intentional infliction of emotional distress...fraud, and other civil causes of action to seek redress,” (emphasis added). In cases where one user utilizes a fake profile to defraud another user—which I’d imagine is the situation in most of these fraud cases—it seems that those legal tools are extremely difficult to use.**

- a. **So how would a user even go about identifying a perpetrator to bring a lawsuit? Can you tell the Committee how many civil cases have even been filed in these situations?**

Response: Parties bringing meritorious lawsuits to identify anonymous Internet users can and frequently do identify the perpetrators of illegal acts. Courts for decades have confronted the

Dr. Corynne McSherry, Ph.D.
Page 7

competing and weighty interests implicated in these cases: the right to obtain evidence and identify perpetrators and First Amendment right to speak anonymously.

The First Amendment protects anonymous speakers, though not absolutely. Our founders believed that anonymous speech was an essential tool to provide critical commentary and to foster public debate. The Supreme Court has recognized that anonymous speech is not some “pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent.” *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 357 (1995). Anonymity is often a “shield from the tyranny of the majority.” *Id.* at 357. “The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one’s privacy as possible.” *Id.* at 341–42. Indeed, our founders relied on anonymity in advocating for independence before the Revolutionary War and later when publishing the Federalist Papers as they debated our founding charter. *See Talley v. California*, 362 U.S. 60, 64–65 (1960).

“Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas. The ability to speak one’s mind on the Internet without the burden of the other party knowing all the facts about one’s identity can foster open communication and robust debate.” *Doe v. 2TheMart.com Inc.*, 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001).

As the court in *Dendrite Int’l v. Doe No. 3*, recognized, procedural protections for anonymous speakers are needed to ensure that litigants do not misuse “discovery procedures to ascertain the identities of unknown defendants in order to harass, intimidate or silence critics in the public forum opportunities presented by the Internet.” 775 A.2d 756, 771 (N.J. App. Div. 2001). Similarly, the court in *Doe v. Cahill* stated, “there is reason to believe that many defamation plaintiffs bring suit merely to unmask the identities of anonymous critics.” 884 A.2d 451, 457 (Del. Sup. Ct. 2005).

Courts have also recognized that, in meritorious cases, parties have a compelling interest to identify anonymous Internet speakers and vindicate legal claims. To balance the competing interests in parties obtaining justice and speakers’ First Amendment rights, courts have developed legal tests that determine when a party is justified in identifying anonymous Internet users. Although the specifics of these tests vary, they generally require the party seeking to identify an anonymous speaker to show early on that their case has merit and that they have endeavored to identify the individual without a court’s help. Upon meeting those tests, parties are generally able to use legal process, such as subpoenas, to obtain identifying information about Internet users and then pursue legal claims against them.

The law as it stands thus already provides a path for individuals to vindicate legitimate legal claims against individuals while also protecting anonymous online speakers from vexatious and harassing lawsuits designed to violate or chill their First Amendment rights. We have not tracked specific numbers, but we see many instances in which the disclosure of pseudonymous and anonymous user data is compelled upon a proper showing by a plaintiff. Of course, there will be examples where it may be very difficult to identify an offender, but that challenge is not unique to the Internet.

Dr. Corynne McSherry, Ph.D.
Page 8

2. Many of us are aware of federal indictments against foreign nationals and U.S. residents for running these scams, which is wire fraud.

a. But how many of the foreign nationals do you believe will see a courtroom, let alone a prison cell?

Response: The answer to that question lies beyond EFF's expertise, but we suspect it involves fundamental issues involving law enforcement resources, complexities of extradition, and cross-border prosecutorial agreements.

b. At what point should an online platform have responsibility to a victim harmed by a user the platform failed to verify?

Response: This will vary greatly according to the situation. But we do not support placing an affirmative duty on platforms to verify every one of their users.

First, given the problem of scale, this will be very difficult to do and very burdensome. We fear that only the most entrenched and best-resources platforms will be able to make even a meaningful effort, much less succeed.

Second, the First Amendment and international human rights laws protect the right to anonymous and pseudonymous speech, with good reason. As noted, our founders relied on anonymity in advocating for independence before the Revolutionary War and later when publishing the Federalist Papers as they debated our founding charter. *See Talley v. California*, 362 U.S. 60, 64–65 (1960). They understood that anonymous speech was an essential tool to provide critical commentary and to foster public debate. Accordingly, the Supreme Court has consistently recognized that anonymous speech is not some “pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent.” *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 357 (1995). That is still true today, when there are many people, such as those living in oppressive regimes abroad or as minorities in their communities in this country, who face dangerous retaliation if they attach their real identities to their speech.

c. Is there a point where a platform's unwillingness or inability to protect consumers make them liable?

Response: Courts, such as the Ninth Circuit in the *Internet Brands* case, have appropriately identified situations in which a platform may owe a duty to its users. This is when the duty arises from something other than a third party's contribution of content to the platform. *See Doe v. Internet Brands, Inc.*, 824 F.3d 846, 848 (9th Cir. 2016).

Platforms could take action if put on notice by user complaints. However, this is problematic due to the “heckler's veto” problem, where some users deploy illegitimate complaints to try to silence other users. At EFF, we have seen many examples of this kind of abuse, such as efforts to flood a platform's takedown systems with takedown complaints/demands, and seen how it can lead to the silencing of legitimate speech, particularly minority voices.

Dr. Corynne McSherry, Ph.D.

Page 9

As for Prof. Citron's duty of care proposal, we fear it does not adequately protect online speech.

First, it is effectively a negligence/reasonableness rule that will inevitably lead to ruinous litigation for smaller platforms as they try to prove that the actions they have taken are adequate. Moreover, if the analysis is largely fact-based, then a defendant will not be able to resolve the litigation quickly and the effectiveness of Section 230's limits on litigation burdens and financial costs is lost. This adds up to a strong incentive to simply over-censor to try to stave off litigation.

Second, duty of care proponents have acknowledged that it would not apply to the largest platforms, because it would not be reasonable for them to take action at scale. Thus, this proposal wouldn't even apply to a vast amount of online content.

Finally, we note that while market pressures already encourage platforms to verify and screen users, any legislation in this area is likely to pose a constitutional problem under the First Amendment.

Ms. Gretchen S. Peters
Page 1

Additional Questions for the Record

**Subcommittee on Communications and Technology and
Subcommittee on Consumer Protection and Commerce
Joint Hearing on
“Fostering a Healthier Internet to Protect Consumers”
October 16, 2019**

Ms. Gretchen S. Peters, Executive Director, Alliance to Counter Crime Online

The Honorable Kathy Castor (D-FL)

1. **On June 19, 2019, The Verge published an investigation into one of Facebook’s content moderation sites in Tampa, FL, which is operated by the firm Cognizant. The article details allegations of appalling working conditions including sexual harassment, verbal and physical fights, theft, and general filthiness in addition to adverse mental health effects associated with the nature of their work.**
 - a. **Operationally, how should tech platforms moderate their content? What role should human content moderators play? What role should technology play?**

Response: Platforms should ban all serious crime activity, and should implement systems to enforce these policies, instead of just stating them. The Alliance to Counter Crime Online believes that Congress should modify existing laws to make tech firms strictly liable for hosting specific criminal and terror content, after the firms have observed the content and refuse or fail to notify law enforcement in the country where the crime is being committed, and that unless and until this happens, many firms will take a lax approach to the issue of toxic content. Firms should implement content-control systems that combine the work of human moderators and AI technology, as well as user generated tips. The last few years have shown that. While artificial intelligence can and does identify a tremendous amount of illegal activity, this identification is futile if action is not taken to stop the actual crimes being committed. The majority of AI-identified criminal content today is simply removed from the platform, and often deleted without being communicated to law enforcement. This is literal destruction of evidence rather than moderation.

There will need to be content moderators, as well as investigative units that patrol the platforms for new trends and issues. Facebook and other firms must also be more strategic in how it invests in moderators. Currently, Facebook’s content moderators do not maintain any expertise in a particular subject area, they are simply “cleaners” for the platform. Many do not even have college degrees, let alone expertise in the intricacies of organized crime and terrorism. If Facebook, and other firms, were to invest in subject matter experts (i.e. terrorism experts, wildlife experts, conflict antiquities trafficking experts) they would not only be more effective at

Ms. Gretchen S. Peters

Page 2

identifying and dismantling illicit content networks, they would also have a team of people that were trained, prepared, and capable of dealing with the heinous content they so routinely encounter.

Firms should be regulated to hand over IP addresses and other identifying data about users engaging in illicit activity on their platforms to law enforcement, much the way banks must file suspicious activity reports (SARs). When a SAR is reported to the government, there should be regulations for how long the firm must hold the data (minimum 1 year) in the event that law enforcement wants to pursue a case. Because crime networks often use multiple platforms at once to mount sophisticated scams and crimes, there should be mechanisms to facilitate and encourage information and data sharing between the large tech firms and law enforcement to coordinate.

b. What standard should a private company use to evaluate content? “Quasi constitutional”, a “community standard” established by the company along the lines of other private media, other?

Response: a “community standard” established by the company along the lines of other private media should be sufficient. Many companies already have perfectly acceptable policies and standards, they just fail to enforce them.

c. Given that private companies are not governed by standards that government would be when it decides not to post content, why do content moderators have to spend so much time reviewing and in such great detail evaluating explicit, violent, or hateful content? What value is there to society and the site owner to work to ensure that such explicit, violent, or hateful content is given every opportunity to be posted?

Response: There is no value to society to this, other than news content reporting on terror attacks, etc (and news content could be tagged so it would not get flagged by AI systems). Companies claim to be careful about moderation in order to avoid violating free speech, however there is no federally mandated system in place to regulate what firms must do once illicit activity has been detected, as there is with the regards to banks and financial firms. This lack of regulation is precisely why the problem has grown to this point.

Firms can and should use AI to block the vast majority of the most violent, toxic and pornographic content, only forwarding that which appears to reflect a violation of the law (e.g. child pornography, drug sales etc.), so that it may be passed to authorities. It is shocking to learn about the extent of animal abuse and torture that occurs on the web, for example. All the major online tech platforms have “community standards” banning violent and explicit content, however many black markets hide inside groups on Facebook and other platforms, where the majority of illicit activity occurs. Moves toward greater encryption by major tech platforms threaten to make this worse, not better. Congress must find a balance between rule of law and user privacy, but the two issues do not need to be mutually exclusive.

Ms. Gretchen S. Peters

Page 3

AI systems on their own will never be enough, because people are smarter than systems, and quickly learn to skirt the settings, unless there are human moderators to evaluate specific instances.

- d. This explicit, violent, or hateful content often is known to be inconsistent with the tech platform's content bylaws. Why do tech platforms, like Facebook, force content moderators to not only look at but also evaluate in great detail explicit, violent, or hateful content that is often inconsistent with the tech platform's bylaws?**

Response: We ask ourselves the same question every day. Could it be that firms like Facebook realize they are earning so much money off this traffic to perceive a reason not to remove the content? We don't know. We propose Congress ask tech firms like Facebook and Google to declare what revenue they get from users who come online and engage with opioid content, for example. What we do know is that every click is a datapoint, and that data has value to Facebook. When alliance researchers identify 100 Facebook groups trafficking blood antiquities, they are looking at groups with a pool of roughly 2 million members. The question to ask Facebook is: "How much is the data of those individuals worth?"

We are of the opinion that Facebook and other tech firms have created a moderation system that, on the surface, appears to be attempting to tackle the issue of illegal and explicit content. However, our research and whistleblowers who have collaborated with us report that this very same system is seemingly intentionally designed to minimize the efficacy of those moderators.

Moderators are given a daily quota of 840 "tickets" (individual flagged items to review) for each 8-hour work day. If the moderators take a 1-hour lunch break, that leaves 7 hours of work available to reach the quota of 840 tickets. On average, the moderators have to observe, investigate, make a decision, and move on to the next ticket in 30 seconds or less in order to reach their quota. This process frequently involves reading through the user's Facebook Messenger inbox to understand the user's general activity. If the moderator decides to escalate a ticket, the moderator has to state a case to his/her supervisor as to why the ticket needs to be escalated, then make a report to a representative from Facebook who will make the final decision as to whether or not the ticket warrants escalating to law enforcement or taking further action. (Based on our sample data, 100% of the time when escalated tickets involve serious illegal activity involving users who are outside of the US and Canada, Facebook has refused to escalate the ticket.) All of this effort takes time away from the 30 second window the moderators have available to stay on track to meet their quota. Additionally, in 30 seconds or less, in all but the most obvious cases it is nearly impossible to sufficiently investigate a user's account and message traffic to understand if serious crime is occurring.

Moderators who fail to meet their daily quota are denied overtime, holidays off, and do not have their contract renewed or are fired before their contract expires. This is an incredible incentive to the moderators not to escalate any items.

Moderators that we have spoken to are graded for their efficiency and accuracy in correctly marking tickets that are either scams or not scams. There is no professional performance metric

Ms. Gretchen S. Peters
Page 4

that measures whether or not moderators remove or escalate content that involves serious criminal activity so long as no scam is occurring.

In other words, if a moderator views 840 tickets all relating to the sale of 7-year-old girls to a known human trafficker, and the moderator believes that the sales are real and are not a scam, the moderator will receive a perfect efficiency rating if the moderator does not mark or escalate any of the 840 tickets.

e. Should content moderators have more leeway to ban harmful content so they don't have to look at it over such lengthy time periods and evaluate the content in such detail?

Response: Yes. In fact, as stated earlier, AI should remove it before they have to see most of it. However, moderators are not spending lengthy time periods evaluating individual cases of graphic content, as they are systematically held to a standard of 30 seconds or less per ticket. If the user posting this damaging content is not banned, the user will continue to post and put moderators in a perpetual game of whack-a-mole. The psychological damage to the moderators comes in the form of a daily onslaught of horrible images and events, made worse by the frequency that the moderators are told that no action will be taken to help the victims in the case or to prosecute the criminals.

The main issue is reporting the serious crime to authorities. Facebook's AI system known as "Sigma" automatically removes a good amount of content that pertains to illegal sale of drugs, however moderators are told that this information does not need to be escalated to law enforcement because Sigma has already removed the content (even if the drug seller and purchaser have already made contact via Facebook.) Our alliance has debriefed multiple Facebook moderators from Cognizant and other firms who describe online "auction groups" where members can pay to be invited to watch video streams of animal torture, child abuse, bestiality, sadistic rituals and other illicit activities. Moderators told us the same people ran groups like these over and over, and even took payment sometimes using Facebook payment systems. But Facebook does not report this activity, or the identities of these users to law enforcement, unless there are children in America in the videos. Animal torture and sadistic activities involving adults may stay up – even when they are in violation of Facebook's own policies. Even if there are American children being abused in those videos, the 30 seconds or less standard of investigation ensures that a great deal of crime, regardless if the victims are American children or foreign children, will go unreported and will not get escalated. This needs to change.

f. What should industry best practices be for treating content moderators? Should Congress play a role in ensuring worker rights in this unique industry? If so, how?

Response: Basic labor law violations appear to be occurring as it relates to failure to pay hourly employees overtime pay for overtime work. These contractors should be reviewed by the Department of Labor to ensure that the employees are being afforded the basic rights of American workers. Moderators are monitored constantly, to the point that their supervisors know

Ms. Gretchen S. Peters

Page 5

precisely how many times and for how long the moderators take bathroom breaks, so the data regarding their hourly and overtime hourly work is available.

Removal of the unreasonably high 840 daily ticket quota will go a long way to ensure that moderators are able to perform their very serious job with the time and attention that each ticket deserves. We are of the opinion that the combination of witnessing traumatic events and the feeling of helplessness associated with regularly being told not to escalate serious crime to law enforcement creates a particular harm to the mental health of the moderators.

Soldiers and police officers deal with very traumatic cases on a regular basis, and while these traumatic events still take their toll, soldiers and police officers experience a tremendous amount of pride and satisfaction in their work. This satisfaction is derived from being able to help others and make a difference. If the moderators are working in an environment where they are actually able to help, then the moderators will experience a similar sense of pride and fulfillment that comes from helping to make a real difference in the world.

Creating a system that rewards moderators for finding information that leads to the arrest of human traffickers, child rapists, and drug traffickers will create a fundamental change in the experience of the moderators, changing from their current experience of trauma and futility, and shifting to an experience where their efforts are able to help the victims that they see in the tickets.

Mental health is a very serious matter, and any job that requires regular and significant exposure to incredibly traumatic content responsibly needs access to professional mental-health care. One moderator that we have spoken to specifically asked to see a psychiatrist to help cope with the graphic content the moderator was being subjected to and their supervisor denied them access to a professional mental health provider.

g. Is it common practice among tech platforms to use contractors to conduct content moderation for their sites? Why do some tech platforms use contractors to conduct content moderation for their sites? Should tech platforms do this?

Response: From what we know about this still-veiled industry, is fairly common practice for tech companies to use contractors for their sites. There are several reasons they might use contractors for what are arguably the most psychologically damaging jobs in tech: 1) It keeps the companies from being liable for the mental health of these employees, 2) it is a cost-cutting measure, hiring contractors at low rates also means the companies do not have to provide health care – an especially pressing issue when considering the emotional and psychological health of the employees.

We are of the opinion that use of contractor firms to moderate content is done specifically to create layers of liability insulation. Based on the disturbing details about how insufficiently the moderators are trained and managed, the objective of Facebook, and other firms, is clearly not to police their platform, arrest criminals, and rescue victims. Rather, the appears to be taking the minimally required action to create the illusion of addressing the issue, while maintaining an

Ms. Gretchen S. Peters
Page 6

arms-length distance between content moderation and regular firm employees. This way Facebook can blame another corporation if and when the gross inadequacy of the moderation efforts become known to the public (and Congress.)

The Honorable Lisa Blunt Rochester (D-DE)

1. What can the federal government do to improve the capacity and ability to effectively moderate online content, including technological research?

Response: The federal government should establish a whistleblower program focused on ensuring compliance with new regulations on illicit and toxic content. Corporate crime is often difficult to detect, and the experience with SEC, CFTC and IRS whistleblower programs is that detection and enforcement is greatly enhanced when whistleblowers are incentivized to step forward. Key elements of this program would include protections against retaliation (including the right to submit evidence to authorities anonymously and confidentiality) and financial rewards to whistleblowers when their information contributes to successful prosecutions and monetary sanctions, so that tech employees and former users of illicit content can receive rewards for coming forward with information. Fines from these programs should be allocated to a fund for law enforcement and for scholarship about illicit and toxic content.

The Honorable Richard Hudson (R-NC)

1. We've heard today that CDA 230 was intended to be both a "sword" as well as a "shield". My colleagues before me have addressed how there are legitimate concerns that the "sword" aspect is somewhat underutilized. Over the last five years we have seen a dramatic increase in terrorist activities online. Social networking sites and other online platforms have been used by terrorist organizations to not only spread their hateful rhetoric but also as a powerful recruiting tool, including inside the United States.

a. Do you believe that online platforms currently do enough to counter the spread of terrorist propaganda online?

Response: We would argue that the "sword" aspect has been almost entirely forsaken by tech firms, who realized they could scale faster if they ignored toxic content. This has allowed terror groups and drug cartels to weaponize social media, using platforms to recruit new members, broadcast their messages on a far wider scale than they could have ever imagined before, and to target victims for threats, extortion and even murder. Facebook's own AI has even *generated* terror content, according to a whistleblower report from May 2019.¹ The company has put so little effort into wielding its "sword," that the same AI technology generated more than 100 business pages for ISIS months after Facebook was questioned on the whistleblower report in a

¹ <https://www.whistleblowers.org/wp-content/uploads/2019/05/Facebook-SEC-Petition-2019.pdf>

Ms. Gretchen S. Peters

Page 7

Congressional hearing.² The company has yet to remove these pages and has not fixed the algorithm that creates them.

Furthermore, members of our alliance have released extensive reporting about how terrorists (confirmed by human intel) are using the platform to actually raise money by selling conflict antiquities – a war crime – on Facebook.³ These alliance members have spoken to officials at Facebook directly about the urgency of these issues, but the company has yet to change its commerce policies to address these concerns. Terrorists are not just spreading propaganda through Facebook, they are using the platform as an outlet for fundraising.

b. Do you believe CDA 230 provides an adequate framework to address this growing issue?

Response: Not at all. Times have changed. When CDA230 was written, the tech industry was in its infancy and most people connected to the Internet over a dial-up telephone. Smartphones and social media had not been invented. Today's technologies allow terrorists and criminals to spread globally at a far faster pace than ever before in history. For the health and safety of the American people, we must remove immunities for hosting criminal content.

If a child was sold into prostitution inside the privacy of a motel room, nobody would think that the owner of the motel or its employees should be prosecuted or liable for the crime of human trafficking. This is in essence what was the intent of CDA 230; that a provider of a legal service should not be liable for the illegal misuse that may be committed by a third party. This makes sense, and nobody would argue the reasonableness of this limitation of liability.

But what if that specific motel is a known and frequented location where child sex trafficking occurs? What if the motel owner and their managers all know for a fact that children are regularly being sold into prostitution inside their motel rooms? What if every single motel room has full video and audio surveillance of every second of human trafficking activity, yet 9 times out of 10 the motel owner and motel managers choose to delete the video evidence and order their employees not to talk about what they saw and not to report it to law enforcement. What if the motel owner and managers are specifically receiving compensation directly related to the prostitution of children on their premises? Does anyone think that the motel owner and managers should still not be held liable?

This second situation is literally what happens on social media platforms. Facebook and Google in particular continue to use CDA 230 to avoid action and responsibility despite their available knowledge, evidence, and capability. This is why CDA 230 must be amended.

² <https://apnews.com/3479209d927946f7a284a71d66e431c7>

³ <http://atharproject.org/wp-content/uploads/2019/06/ATHAR-FB-Report-June-2019-final.pdf>

Ms. Katherine Oyama
Page 1

Additional Questions for the Record

**Subcommittee on Communications and Technology and
Subcommittee on Consumer Protection and Commerce
Joint Hearing on
“Fostering a Healthier Internet to Protect Consumers”
October 16, 2019**

Ms. Katherine Oyama, Global Head of Intellectual Property Policy, Google, Inc.

The Honorable Anna G. Eshoo (D-CA)

- 1. Many of the issues raised today are serious ones that we, as a society, need to work to resolve. How is Google working on these issues today? One example I’m especially worried about is how you deal with the sales of illegal opioids on your platforms today. How does Section 230 play a role in those practices?**

Response: The opioid epidemic is complex and tragically historic, and many organizations and families are working to find solutions. Google has been doing its part specifically to help support efforts relating to prevention, treatment, and recovery. Google is supportive of legislative approaches to increase user awareness about the dangers of opioids, and provide resources to people with substance use disorders, and their families, with help for treating addiction and remaining in recovery. Google actively promotes prescription drug take back programs, like the DEA’s Rx Take Back Day in April and October, as well as permanent disposal efforts run by pharmacies (e.g., CVS, Riteaid, Walgreens, and hospitals) or municipalities (law enforcement), to lessen the risk that legitimate, but unused prescriptions are diverted for misuse.

Google also has a number of efforts to combat the sales of illicit drugs, including illegal opioids, across our platforms. Such content is strictly against many of our products’ policies, such as Ads and YouTube. Google regularly removes policy-violating content relating to controlled substances, including opioids, from its ads platforms and YouTube (with the help of a third party, Legitscript, and our internal manual/automated filters). In March 2020, our Ads platforms will begin blocking marketing of opioid painkillers generally.

- On Web Search, our approach is two-fold. Most links to purported offers to sell opioids without an Rx are actually non-delivery scams. Google has undertaken extensive efforts to combat those listings (e.g., over 2 billion opioid-related spam listings were actioned, delisted or heavily demoted).
- In Spring 2018 we began to work with the FDA to delist--in other words, remove from search results--websites that are the target of an FDA Warning Letter for purporting to sell opioids without a prescription. We have removed hundreds of sites under this process.

Ms. Katherine Oyama

Page 2

Queries seeking information about opioids and treating addiction are much more common than "buy [opioid]" queries by many orders of magnitude. On our Ads platform, we have also taken efforts to prevent abusive addiction treatment advertisements, particularly by patient brokers.

We are able to take these actions precisely because of CDA 230's incentives for responsible content moderation efforts. The law's "good samaritan" provisions were designed to incentivize self-monitoring and facilitate content moderation. Without it, we could not have the types of rigorous policies and programs that we have in place to defend against misuse of our platforms.

The Honorable Kathy Castor (D-FL)

1. **On June 19, 2019, The Verge published an investigation into one of Facebook's content moderation sites in Tampa, FL, which is operated by the firm Cognizant. The article details allegations of appalling working conditions including sexual harassment, verbal and physical fights, theft, and general filthiness in addition to adverse mental health effects associated with the nature of their work.**
 - a. **Operationally, how should tech platforms moderate their content? What role should human content moderators play? What role should technology play?**

Response: Our strategy for tackling illegal and potentially harmful content is tailored to each of our platforms. For each of our products, we have a specific set of rules and guidelines that are suitable for the type of platform, how it is used, and the risk of harm associated with it.

We use a mix of machines and people to enforce our policies at scale. Machine learning is allowing us to identify and remove violative content faster than ever before, and our investment in technology enables us to address enforcement of our content policies at scale. For instance, on YouTube, over 93% of videos removed for violating our policies in the third quarter of 2019 were first detected and flagged by our automated detection systems.

However, while machine learning is good at examining large sets of data and looking for content similar to previously removed material, the technology is still evolving. It cannot perfectly identify all violations, and, in general, people are better at making the nuanced, context specific judgments that are often necessary when it comes to evaluating speech and other expression. When videos are flagged by our machines, they are then sent to our trained teams of reviewers, who can analyze the content and take quick action. In many cases, we are able to take action before content has been viewed or accessed by anyone; for instance, during the third quarter of this year, nearly 68% of videos on YouTube that were first flagged by machines were removed before a single view.

Together, this work represents a significant investment. We have over 10,000 people across

Ms. Katherine Oyama
Page 3

Google working on content moderation and removal on our platforms and have invested hundreds of millions of dollars in these efforts.

b. What standard should a private company use to evaluate content? “Quasi constitutional”, a “community standard” established by the company along the lines of other private media, other?

Response: Across our products, we develop ‘rules of the road’ – known as ‘content policies’ or ‘community guidelines’ – which outline what types of content and behaviors are acceptable on each product or service. We aim to make them abundantly clear to all users and content creators and ensure they are easily accessible.

They articulate the purpose and intended use of a given product or service and represent what makes that product unique. They also explain what types of content and behaviors are not allowed and the process by which a piece of content or its creator may be removed from the service

To that end, YouTube’s Community Guidelines prohibit certain categories of material, including sexually explicit content, spam (such as videos trying to trick people to ‘click through’ to another site), hate speech, harassment and incitement to violence. In evaluating videos, we consider purpose and context, including allowing content in some cases if the purpose is educational, documentary, scientific, or artistic in nature. If users are posting content related for this purpose, for instance, we encourage them to be mindful to provide enough information so viewers understand the context, such as through an introduction, voiceover commentary, or text overlays, as well as through a clear title and description. Providing documentary or educational context can help the viewer, and our reviewers, understand why potentially disturbing content sometimes remains live on YouTube.

Sometimes, we make mistakes in our decisions to enforce our policies, which may result in the unwarranted removal of content from our services. To address that risk, wherever possible, we make it clear to creators that we have taken action on their content and provide them the opportunity to appeal that decision. The decision will then be evaluated by a different member of our trust and safety team.

c. Given that private companies are not governed by standards that government would be when it decides not to post content, why do content moderators have to spend so much time reviewing and in such great detail evaluating explicit, violent, or hateful content? What value is there to society and the site owner to work to ensure that such explicit, violent, or hateful content is given every opportunity to be posted?

Response: YouTube is built on the premise of openness. Based on this open platform, millions of creators around the world have connected with global audiences and many of them have built thriving businesses in the process. But openness comes with its challenges, which is why we also have Community Guidelines that we update on an ongoing basis. Most recently, this includes our hate speech policy and our upcoming harassment policy. When you create a place designed

Ms. Katherine Oyama
Page 4

to welcome many different voices, some will cross the line. Bad actors will try to exploit platforms for their own gain, even as we invest in the systems to stop them. As discussed above, we rely on a combination of people and technology to flag inappropriate content and enforce our Guidelines. We continue to improve not only our enforcement processes, but also our policies over time; for instance, in the last year, we made significant improvements to our policies around hate speech and harassment. Problematic content represents a fraction of one percent of the content on YouTube and we're constantly working to reduce this even further.

d. This explicit, violent, or hateful content often is known to be inconsistent with the tech platform's content bylaws. Why do tech platforms, like Facebook, force content moderators to not only look at but also evaluate in great detail explicit, violent, or hateful content that is often inconsistent with the tech platform's bylaws?

Response: At YouTube, our Community Guidelines prohibit incitement to violence, hate speech, and graphic content, among other categories of content. And we continue to tighten our policies on what content can appear on our platform, or earn revenue for creators.

We've increased our enforcement teams and invested in powerful new machine learning technology to scale the efforts of our human moderators to take down videos and comments that violate our policies. Human reviewers remain essential to both removing content and training machine learning systems because human judgment is critical to making contextualized decisions on content.

Context is very important for all videos, but it's particularly important when evaluating these categories of content -- and we must be careful to assess potential educational, scientific, newsworthy, or a documentary content that is allowed on YouTube if it includes context. Human moderators have an important role in recognizing contextual nuances.

This context-sensitive approach is important to maintaining the benefits of YouTube as an open platform. Based on this open platform, millions of creators around the world have connected with global audiences and many of them have built thriving businesses in the process. If we were to take the approach of merely relying on automated approaches to relying on content, we would risk over-removing and limiting access to legitimate, non-violative speech.

e. Should content moderators have more leeway to ban harmful content so they don't have to look at it over such lengthy time periods and evaluate the content in such detail?

Response: The context in which a piece of content is created or shared is an important factor in any assessment about its quality or its purpose. We are attentive to educational, scientific, artistic, or documentary contexts, where the content might otherwise violate our policies. This work can be emotionally challenging, especially when the people who review the content against our policies are exposed to some of the most shocking or abhorrent types of content

Ms. Katherine Oyama
Page 5

that exist online. Google is determined to support the wellness of these workers through high wellness standards, verification of vendors' compliance with those standards, and research & technological innovation to promote wellness and mitigate trauma caused by content moderation.

f. What should industry best practices be for treating content moderators? Should Congress play a role in ensuring worker rights in this unique industry? If so, how?

Response: YouTube works closely with our vendor partners to ensure a standardized, comprehensive wellness program is delivered to all agents reviewing sensitive content. All agents have access to onsite counseling services, wellness breaks, resilience training, and organized wellness activities to ameliorate the mental health impact of reviewing sensitive content. We are competitive in the space of compensation and continue to evaluate pay relative to industry standards, and ensure those who are reviewing more sensitive content are compensated accordingly.

g. Is it common practice among tech platforms to use contractors to conduct content moderation for their sites? Why do some tech platforms use contractors to conduct content moderation for their sites? Should tech platforms do this?

Response: While we cannot speak to the practices of other companies, content moderation at Google and YouTube is primarily managed by Trust & Safety teams that sit across the company. These teams work with our in-house legal and policy departments on escalations and also oversee the vendors we hire to help us scale our operations. These teams are made up of engineers, content reviewers, and others who work across Google to address content that violates any of our policies. They are made up of a mix of full-time employees and contractors.

The Honorable Lisa Blunt Rochester (D-DE)

1. At the October 16, 2019, joint hearing, you provided commitments that Google will disclose information on diversity of your content moderators and issues with hiring diverse content moderator teams. Please provide that information to the Energy and Commerce Committee and my office.

Response: As you may know, Google was the first large technology company to publish workforce diversity data in 2014 (all of this information is available at [google.com/diversity](https://www.google.com/diversity)). We are committed to sharing our numbers every year, and 2019 was no different. We provide one of the most transparent data sets in our industry and our report allows the public to view a demographic representation of our employees, toggle between different job functions & leadership roles, and even view this data intersectionality. Beyond diversity of race and gender, we also included veterans, people with disabilities, and LGBTQ people in this data for the first time last year. To your question, the Google moderators are a mix of tech and non-tech employees who are representative of Google as a whole. Our 2019 Diversity Annual

Ms. Katherine Oyama

Page 6

Report can be found at <https://diversity.google/annual-report/>.

We believe it is important to be transparent about our challenges and key learnings in this arena. Our original decision to release our workforce (diversity) numbers led to other companies following suit. Google stands firm in its commitment to foster dialogue and to drive impact on this important issue.

2. What can the federal government do to improve the capacity and ability to effectively moderate online content, including technological research?

Response: Our strategy for tackling illegal and harmful content is tailored to each of our platforms. Across our products, our teams tackle a huge spectrum of online abuse, from scams, like the email from a ‘relative’ stranded abroad needing a bank transfer to get home safely, to abhorrent content, including child sexual abuse material (CSAM) online.

It is important to note, however, that rogue, off-shore sites that promote illegal and harmful activity are often commercial in nature -- they’re running scams or selling illegal goods to make a profit. A critical way to stop these sites is to cut off their money supply (i.e. payments processors, advertising services, etc.). Removing the site from Search, for example, doesn’t remove it from the Web, but money is the oxygen that many bad actors need to survive. Cut that off, and many of them will go away.

Furthermore, CDA 230’s civil law framework does nothing to alter existing law enforcement tools and liability framework for violations of federal criminal laws, which are expressly exempted from the scope of the Communications Decency Act. This is why combating difficult problems of illegal content requires a response from government, individuals, and organizations, often working in partnership. We stand ready to work in concert on these issues.

The Honorable Tom O’Halleran (D-AZ)

1. Ms. Oyama, as written in statute, Section 230 has “good Samaritan” language to incentivize online platforms to take actions “*in good faith to restrict access to or the availability of*” harmful content.

Many platforms have established content or use of service policies to specify what behavior is allowed by the service, while others employ artificial intelligence formulas to automatically filter user-generated content. Some platforms also hire human content moderators to review and remove content posted by users on its platforms that is considered harmful, violent, or graphic. These content reviewers often suffer from Post-Traumatic Stress Disorder (PTSD).

Ms. Katherine Oyama
Page 7

a. What more can be done by the government and industry to ensure sufficient mental health services are made available to human content reviewers?

Response: YouTube works closely with our vendor partners to ensure a standardized, comprehensive wellness program is delivered to all agents reviewing sensitive content. All agents have access to onsite counseling services, wellness breaks, resilience training, and organized wellness activities to ameliorate the mental health impact of reviewing sensitive content. We are competitive in the space of compensation and continue to evaluate pay relative to industry standards, and ensure those who are reviewing more sensitive content are compensated accordingly.

The Honorable Greg Walden (R-OR)

1. At the hearing, Rep. Bilirakis asked EFF whether they have argued for including language mirroring legislation in trade deals explicitly for the purpose of “baking” language into an agreement to protect the statute domestically.

For the record, Yes or No: Is including such 230-like language in trade agreements an attempt to preclude us – the committee of jurisdiction – from revisiting the statute? Do you see the intent of including such 230-like language in trade agreements is to ensure that we may not revisit the statute?

Response: No.

2. During the hearing, you mentioned that Google has a tool to tag copyrighted works so that upon re-upload they can be stopped before spreading, in the case of illegal content like violent extremism. Can that tool be more widely deployed, both across different platforms, like Reddit, and to cover more content besides copyrighted works? If not, why not?

Response: Google offers a wide range of services on many platforms. Our strategy and technologies for tackling illegal and harmful content can differ based on the nature of the services and the technology of the platforms. There is no one size fits all approach in these matters. Generally speaking, in addition to content flagged by our users, we develop and deploy cutting-edge technology to proactively identify, remove, and block offending content. In addition, across our products, our human review teams tackle a huge spectrum of online abuse, from scams, like the email from a ‘relative’ stranded abroad needing a bank transfer to get home safely, to abhorrent content, including child sexual abuse material (CSAM) online.

That said, we work with other companies in the industry where we can. For example, in the CSAM space, for over a decade we have been using PhotoDNA, along with other complementary systems, to identify, remove, and report copies of CSAM present in still images and share the digital fingerprints, or ‘hashes.’ We contribute new hashes to, and receive hashes from other platforms via a hash database maintained by NCMEC. In 2015,

Ms. Katherine Oyama
Page 8

YouTube engineers created CSAI Match, which can be used to identify uploaded videos that contain known CSAM. It is used for videos uploaded to YouTube and on Livestreams. CSAI Match is used by companies and organizations like Adobe, Reddit, Tumblr, among others. Building on our previous work to develop and extend machine learning systems, and share technology with industry in 2018, Google engineers launched the Content Safety API. This tool helps us to find and report new CSAM that was not possible using hash matching alone. It also allows us to identify CSAM at scale, by prioritizing for manual review content most likely to constitute CSAM. We make this technology available for free to industry and NGO partners.

- a. **In a response to Rep. Walberg, you pointed to Content ID as one tool Google uses for piracy on its platform. Understanding Section 230 immunity already has an exception for intellectual property in statute, we are interested in better understanding how these tools could be applied to other types of content on Googles' platforms in situations where such content is either criminally illegal (and therefore not covered by section 230) or "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable."**

Are there any other tools for copyrighted content that Google uses besides Content ID, Content Verification Program, or Content Match? If so, please provide the name and a short description of how the tool operates.

Response: Google's approach to combating piracy and illegal content on its platform goes beyond just the use of individual tools and policies. Rather, we believe that successfully decreasing incidents of copyright infringement involves a multi-pronged approach:

1. Create More and Better Legitimate Alternatives

Piracy often arises when consumer demand goes unmet by legitimate supply. The best way to battle piracy is with better, more convenient, legitimate alternatives to piracy, which can do far more than attempts at enforcement can. By developing products with compelling user experiences like Google Play Music and YouTube, Google helps drive revenue for creative industries and steer people toward legitimate alternatives. Google also supports the larger ecosystem by providing the cloud infrastructure that other legitimate services depend on to deliver fast, reliable streaming to their customers.

2. Follow the Money

Rogue sites that specialize in online piracy are commercial ventures, which means that one effective way to combat them is to cut off their money supply. Google is a leader in rooting out and ejecting rogue sites from our advertising and payment services, and we help establish best practices across the industry.

3. Be Efficient, Effective, and Scalable

Ms. Katherine Oyama

Page 9

Google strives to implement anti-piracy solutions that work at scale. For example, as early as 2010, Google began making substantial investments in streamlining the copyright removal process for search results. As a result, these improved procedures allow Google to process copyright removal requests for search results at the rate of millions per week.

4. Guard Against Abuse

Fabricated copyright infringement allegations can be used as a pretext for censorship and to hinder competition. Google is committed to ensuring that it detects and rejects bogus infringement allegations, such as removals for political or competitive reasons, even as it battles online piracy

5. Provide Transparency

Google is committed to providing transparency. In our external Transparency Report, Google discloses the number of requests it receives from copyright owners and governments to remove information from its services to inform ongoing discussions about online content regulation.

For more information, our 2018 "[How Google Fights Piracy](#)" report explains the programs, policies, and technology we put in place to combat piracy online and ensure continued opportunities for creators around the world.

b. I understand Google makes Content ID available to companies that, “own exclusive rights to a substantial body of original material that is frequently uploaded by the YouTube user community.” Can you please describe how Google determines what qualifies as a “substantial body?”

Response: Content ID access requires users to make a certain level of operational investment, without which other rights holders could have their rights impaired and lawful expression could be inappropriately impacted. We maintain [minimum standards](#) for Content ID access to preserve accuracy and quality and evaluate candidates on an individual basis. Some of the factors we consider when matching a rightsholder to one of the tools in our copyright management suite are:

- Whether the company or rightsholder holds exclusive copyrights in their content. Often different entities own broadcast rights, physical resale, and online distribution rights and we must take instructions from the entity that controls online distribution rights.
- Whether the company or rightsholder has a history of sending YouTube complete and valid copyright takedown requests to remove allegedly infringing content.
- Whether the company or rightsholder owns the rights to a variety of content that’s frequently uploaded to YouTube. There is no set requirement for the number of uploads of a rightsholder’s content that must have occurred to grant access, but we

Ms. Katherine Oyama
Page 10

have found that those with significant experience managing their content on the platform are most able to navigate the complexity of copyright licensing on Content ID.

- i. What is the threshold to qualify for Content ID? Is it measured in number of copyrighted rights, the value of those rights, the amount of ad revenue those rights bring to Google's platform, or another metric? If "other," please elaborate on what that metric is.**

Response: As discussed in the previous question, Content ID access requires users to make a certain level of operational investment, without which other rights holders could have their rights impaired and lawful expression could be inappropriately impacted. We maintain [minimum standards](#) for Content ID access to preserve accuracy and quality and evaluate each individually. However, neither "the value of those rights", nor "the amount of ad revenue" play a factor in the evaluation.

That said, YouTube endeavors to make Content ID available to as many rightsholders as possible without sacrificing accuracy and quality. We have found that even major rightsholders can mismanage Content ID, however, resulting in unfair or inaccurate claims on legally-uploaded content. Thus, we try to ensure that we grant Content ID to responsible, enterprise-scale rights holders committed to training and management of the powerful tool. For creators and rightholders who require more simplified copyright tools, we've developed the Copyright Match Tool and the Content Verification 1 Program.²

YouTube's recently launched a Copyright Match Tool, which uses the power of the Content ID matching system to find re-uploads of creator videos on YouTube. Instead of uploading a reference file to YouTube, creators that upload a video to YouTube are shown subsequent uploads of their videos. Creators and content owners can then review the matching videos and file bulk takedowns for any they wish to remove. They can also choose to contact the uploader. In this way, creators remain in control of the works they create on YouTube. This new tool greatly simplifies copyright management so that creators can focus their time on making great videos.

¹ Available at <https://support.google.com/youtube/answer/7648743> .

² Available at <https://support.google.com/youtube/answer/6005923?hl=en> .

- ii. I understand that Google allows some aggregators access to Content ID, and encourages some smaller content creators that Google determines does not qualify for access to Content ID to hire an aggregator. Why?**

Response: We have found that creators often prefer to have an experienced aggregator that specializes in this work to manage it, which can be complex and time-consuming. There is also a significant investment in initially learning how to use copyright management systems appropriately. YouTube offers certification courses to train individuals on the use of Content

Ms. Katherine Oyama
Page 11

ID. We have found that those who are not certified are at much greater risk of making mistakes which can have a significant negative impact on other rightsholders and creators. Even after certification, Content ID requires daily engagement to resolve complex issues.

In addition, in many cases, creators, such as independent musicians, may have already assigned their rights to a music label or hired an aggregator in order to distribute their works on other platforms such as Spotify or iTunes. Despite this, we often learn that a small creator is unaware that an aggregator is already representing their rights on YouTube.

1. Must this aggregator have, “exclusive rights” to their clients’ content, or does Google make an exception for aggregators?

Response: There is no requirement that the aggregator own exclusive rights to a client’s works. The client must own the right to manage the work online and is free to designate the aggregator to represent those rights.

3. We get caught up talking a lot about scale and resources in the conversation about litigation risk from modifying Section 230. One of the benefits of scale, as Google has shown time and again, is that vast amounts of data is needed to create more sophisticated machine learning and algorithms. Do you see the hundreds of hours of video uploaded to YouTube every minute as an asset to be testing the types of technologies Dr. Farid mentions in his testimony?

Response: As with all technologies, the real hard work is in turning raw machine learning models into great products and features that solve problems. Data is just one of many important factors in developing a smart and useful model. Quantity of data is not the main key to success. In fact, with worldwide reach, standardized technology and communications protocols, and rapid price decreases in things like cloud platforms and storage, data has become easy to obtain and create. In fact, large quantities of data can even be paralyzing if not properly understood. Success in machine learning, as in almost any other area of tech, requires selection and execution. Data quality often counts way more than data quantity.

Beyond the data that defines what machines learn, there is a great deal of work to be done in how machines learn. Lots of researchers are looking to find ways for machines to learn effectively with smaller amounts of data. Google has a big interest in addressing this open question of research - we would benefit a great deal if machines learned faster with less data. This is why we have made datasets available for others to train their own models upon -- for example our [Open Images Dataset](#) or our [AVA Video Dataset](#) for Human Action Understanding which we used in training some of our own machine learning models.

4. When law enforcement provides information of actual criminal activity, should platforms be required to act to remove it? How quickly should they respond, and should that vary by provider, for example should smaller providers have more time to respond?

Ms. Katherine Oyama
Page 12

Response: Google appreciates that law enforcement agencies face significant challenges in protecting the public against crime and terrorism. We engage in ongoing dialogue with law enforcement agencies to understand the threat landscape and respond to threats that affect the safety of our users and the broader public.

While we cannot speak for other companies, courts and government agencies around the world regularly request that we remove information from Google products. Government bodies ask us to remove or review content for many reasons. Some requests allege defamation, while others claim that content violates local laws. The laws surrounding these issues vary by country/region. Since each request can differ greatly, our teams evaluate and review the content in context in order to determine whether or not content should be removed due to violation of local law or our content policies. We release a transparency report on these requests which can be found [here](#).

5. Does the Google Play store need section 230 protections, or because you only allow developers/apps in the Play store that meet your Terms of Service, you could create accountability within that portion of Google without Section 230?

Response: The Play Developer Distribution Agreement and incorporated Developer Program Policies do give Google the right to determine what content we do and don't want on Play and to take action against apps and developers that don't meet those policies. And while we rely on the agreement and policies in taking action, CDA 230 remains an important part of enforcing our rigorous policies and programs. Section 230 helps ensure that when we take action against a developer or an app (or remove an app, which might otherwise lead to legal complaints from users), we don't end up in years of litigation with costly discovery. The protections that 230 affords makes it possible for us to have the types of rigorous policies and programs that we have in place to defend against misuse of our platforms.

6. Recently, Mark Zuckerberg said Facebook's size is the only reason it can effectively fight election interference, citing that, quote

"it's why Twitter can't do a good of job as we can...I mean, they face, qualitatively, the same types of issues. But they can't put in the investment. Our investment on safety is bigger than the whole revenue of their company."

He's right, size matters, and we expect a lot more from those who have a "bigger sword." In your estimation, is Google doing enough to earn it's 230 protection?

Response: We cannot speak for Mr. Zuckerberg, but at Google, we know that combating difficult problems of illegal content requires a response from government, individuals, and organizations, often working in partnership. We have not waited for legislation to act in tackling illegal or harmful content. We are committed to doing our part.

Our strategy for tackling illegal and harmful content is tailored to each of our platforms. Across our products, our teams tackle a huge spectrum of online abuse, from scams, like the email from a 'relative' stranded abroad needing a bank transfer to get home safely, to

Ms. Katherine Oyama
Page 13

abhorrent content, including child sexual abuse material (CSAM) online.

For each product, we have a specific set of rules and guidelines that are suitable for the type of platform, how it is used, and the risk of harm associated with it. These approaches range from clear community guidelines, with mechanisms to report content that violates them, to increasingly effective artificial intelligence (AI) and machine learning that can facilitate removal of harmful content before a single human user has been able to access it to blocking and removing content when we are notified that a video violates our guidelines. We now have over 10,000 people across Google working on content moderation and removal on our platforms and have invested hundreds of millions of dollars in these efforts.

The Honorable Richard Hudson (R-NC)

1. **One of the best parts of my job is having the privilege of representing the brave men and women who are stationed at Fort Bragg. Additionally, my district represents one of the fastest growing veteran populations in the country. I take it as my responsibility to advocate for them in everything I do. As you all are aware, the opioid epidemic is something that has ravaged our country and disproportionately affected veterans. One of the underlying issues in this area is the availability of these drugs and how easy it can be for an individual to gain access to them. Unfortunately, we have seen that these drugs are often available through illegal online sales that help fuel this crisis.**

- a. **Can you please explain how your company monitors content on your platform to ensure the illegal sale of opioids does not occur?**

Response: The opioid epidemic is complex and tragically historic, and many organizations and families are working to find solutions. Google has been doing its part specifically to help support efforts relating to prevention, treatment, and recovery. Google is supportive of legislative approaches to increase user awareness about the dangers of opioids, and provide resources to people with substance use disorders, and their families, with help for treating addiction and remaining in recovery. Google actively promotes prescription drug take back programs, like the DEA's Rx Take Back Day in April and October, as well as permanent disposal efforts run by pharmacies (e.g., CVS, Riteaid, Walgreens, and hospitals) or municipalities (law enforcement), to lessen the risk that legitimate, but unused prescriptions are diverted for misuse.

Google also has a number of efforts to combat the sales of illicit drugs, including illegal opioids, across our platforms. Such content is strictly against many of our products' policies, such as Ads and YouTube. Google regularly removes policy-violating content relating to controlled substances, including opioids, from its ads platforms and YouTube (with the help of a third party, Legitscript, and our internal manual/automated filters). In March 2020, our Ads platforms will begin blocking marketing of opioid painkillers generally.

- On Web Search, our approach is two-fold. Most links to purported offers to sell opioids without an Rx are actually non-delivery scams. Google has undertaken

Ms. Katherine Oyama
Page 14

extensive efforts to combat those listings (e.g., over 2 billion opioid-related spam listings were actioned, delisted or heavily demoted).

- In Spring 2018 we began to work with the FDA to delist--in other words, remove from search results--websites that are the target of an FDA Warning Letter for purporting to sell opioids without a prescription. We have removed hundreds of sites under this process.

Queries seeking information about opioids and treating addiction are much more common than "buy [opioid]" queries by many orders of magnitude. On our Ads platform, we have also taken efforts to prevent abusive addiction treatment advertisements, particularly by patient brokers.

b. When you find such content on your platform, do you engage law enforcement in addition to removing the content from your platform?

Response: Google is proud to work with the FDA, the DEA, and other regulatory and law enforcement agencies involved in enforcing laws and regulations concerning the sale of illicit drugs online. Over the past few years, Google has referred thousands of potential rogue pharmacies to law enforcement, including the FDA's Office of Criminal Investigations and, more recently, the DEA's Special Operations Division (to whom we have sent a number of referrals this year alone). We have also referred to the FDA pharmaceutical advertisers who have sought to evade Google's filters for prescription drug advertisements. Google also takes a proactive role in assisting the FDA and other law enforcement agencies in investigative efforts. For instance, in October 2012, Google voluntarily participated in the successful "Operation Pangea V", in which the FDA, in partnership with international regulatory and law enforcement agencies, as well as other companies around the world, took collective action against more than 4,100 internet pharmacies online.

The Honorable Tim Walberg (R-MI)

1. **In response to one of my questions during the hearing, you talked about Google's risk engine and how it is very, squarely in-line with Google's interest to not serve ads next to illegal activity. Indeed, you go on to say, "our advertisers only want to be serving good ads to good content," additionally mentioning that over 2 billion ads are stricken every year, "before they're able to ever hit any page...": making the point that you can do so at scale. This of course, makes sense, given this is where Google makes its money. But if Google has proven it can identify harmful or illegal content in the ads space to protect its bottom line, why then can't Google apply this same process to:**
 - a. Search
 - b. Images

Ms. Katherine Oyama
Page 15

- c. **YouTube**
- d. **Google News**
- e. **Google Assistant**
- f. **Groups**

Response: Our strategy for tackling illegal and potentially harmful content is tailored to each of our platforms. For each of our products, we have a specific set of rules and guidelines that are suitable for the type of platform, how it is used, and the risk of harm associated with it. These approaches range from clear policies and community guidelines, with mechanisms to report content that violates them, to increasingly effective artificial intelligence (AI) and machine learning that can facilitate removal of harmful content before a single human user has been able to access it. We also now have over 10,000 people across Google working on content moderation and removal on our platforms and have invested hundreds of millions of dollars in these efforts.

We use a mix of machines and people to enforce our policies at scale. Machine learning is allowing us to identify and remove violative content faster than ever before. And our investment in technology enables us to address enforcement of our content policies at scale. Machines flag suspect videos for review by trained teams, who can analyze the content and take quick action. This system has had a major impact on the way we tackle harmful content, and has helped our human reviewers remove content more quickly.

Dr. Hany Farid
Page 1

Additional Questions for the Record

**Subcommittee on Communications and Technology and
Subcommittee on Consumer Protection and Commerce
Joint Hearing on
“Fostering a Healthier Internet to Protect Consumers”
October 16, 2019**

Dr. Hany Farid, Professor, University of California, Berkeley

The Honorable Anna G. Eshoo (D-CA)

- 1. Platforms have been criticized for doing too much moderation (particularly with respect to political biases) as well as doing too little moderation (particularly with respect to streaming of mass shootings). Which criticism, if any, is more accurate?**

Response: Although these criticisms are not mutually exclusive, I don't believe that the data supports both claims.

There is significant evidence that online platforms are not doing enough to remove child sexual abuse material, terrorism and extremism material, dangerous and deadly conspiracy theories, dis- and mis-information campaigns, and the sale and distribution of deadly drugs, weapons, and the illegal animal trade. At the same time, there is little evidence – beyond anecdotal – that online platforms are moderating with a systematic political bias.

The Honorable Kathy Castor (D-FL)

- 1. On June 19, 2019, The Verge published an investigation into one of Facebook's content moderation sites in Tampa, FL, which is operated by the firm Cognizant. The article details allegations of appalling working conditions including sexual harassment, verbal and physical fights, theft, and general filthiness in addition to adverse mental health effects associated with the nature of their work.**
 - a. Operationally, how should tech platforms moderate their content? What role should human content moderators play? What role should technology play?**

Response: The issue of horrific working conditions for Facebook moderators is not new, and dates back at least two years – see, for example:

Dr. Hany Farid

Page 2

“The Impossible Job: Inside Facebook’s Struggle to Moderate Two Billion People” by Jason Koebler and Joseph Cox, published in *Vice* on August 23, 2018.

“Scouring Facebook for disturbing content: How risk to moderators is raising concerns” by Davider Mever, published in *ZDNet* in on March 28, 2017.

Because the technology sector has not invested enough in developing automatic algorithms for content moderation (except in the case of copyright infringement, as mandated by U.S. law, and legal adult pornography, as needed to appease advertisers), human moderation remains necessary. Despite rapid advances in artificial intelligence and machine learning, it remains likely that even with significant investments in automated technology, human moderators will remain necessary for years to come.

Facebook is fond of citing their 30,000 moderators as evidence of their commitment to moderating their platform. While this number may sound impressive, it is almost well below the number of moderators that Facebook needs. According to [1], across major US cities, there are an average of 50 employees and officers per 10,000 citizens, yielding a law enforcement to citizen ratio of 1:200. There are approximately 2.3 billion active monthly Facebook users and according to Facebook they have 30,000 moderators. Let’s be generous and say that they have another 10,000 Facebook employees who work as part of the safety/integrity team. This yields a safety to user ratio of around 1:60,000. This is a factor of 300 times less than how we police our streets. It is clear from these numbers and from reports on how overwhelmed moderators are, that Facebook has not committed nearly enough resources to manage their services.

Facebook, and the other technology giants, must invest significantly more into technology to automatically moderate their platforms with the goal of reducing the burden placed on human moderators that are now viewing some of the most horrific and vile content for upwards of 10 hours per day. At the same time, the industry must establish more humane working conditions for these workers or have them mandated by Congress. And, the industry must stop out-sourcing this work and treat these moderators the same way that they do their cherished engineers.

[1] <https://www.governing.com/gov-data/safety-justice/law-enforcement-police-department-employee-totals-for-cities.html>

b. What standard should a private company use to evaluate content? “Quasi constitutional”, a “community standard” established by the company along the lines of other private media, other?

Response: The standard is and should be terms of service / community standards. Facebook and YouTube routinely ban constitutionally protected speech – most notably legal adult pornography – as is their right.

c. Given that private companies are not governed by standards that government would be when it decides not to post content, why do content moderators have to spend so much time reviewing and in such great detail evaluating explicit, violent, or hateful content? What value is there to society and the site owner to work to ensure that such explicit, violent, or hateful content is given every opportunity to be posted?

Dr. Hany Farid
Page 3

Response: There is no inherent value. This is not an issue of freedom of speech or expression. The issue is that taking down content is bad for business and so these companies create absurdly complex, contradictory, and constantly changing rules in attempt to take down as little content as possible while feigning concern for freedom of speech. This is not a speech issue (as seen by their aggressive and effective of adult pornography) – it is simply an economic issue. Let's stop pretending otherwise.

- d. This explicit, violent, or hateful content often is known to be inconsistent with the tech platform's content bylaws. Why do tech platforms, like Facebook, force content moderators to not only look at but also evaluate in great detail explicit, violent, or hateful content that is often inconsistent with the tech platform's bylaws?**

Response: Please see response to part (c).

- e. Should content moderators have more leeway to ban harmful content so they don't have to look at it over such lengthy time periods and evaluate the content in such detail?**

Response: Yes. Facebook and the like could create much simpler and easier to enforce guidelines which would in turn make content moderation easier to implement. This, however, runs against their core business model and so I am not optimistic that they will change their practice without significant public or regulatory pressure.

- f. What should industry best practices be for treating content moderators? Should Congress play a role in ensuring worker rights in this unique industry? If so, how?**

Response: I am not an expert in worker's rights, but this is an important question. I believe that Congress should act to protect workers because the technology sector has shown over the past two decades that they are not able to self-regulate and that they routinely put profit and growth ahead of all else.

- g. Is it common practice among tech platforms to use contractors to conduct content moderation for their sites? Why do some tech platforms use contractors to conduct content moderation for their sites? Should tech platforms do this?**

Response: I am only aware that Facebook out-sources most of their content moderation. I am not aware of how Google/YouTube or Twitter employ their moderators. I cannot say for sure why Facebook out-sources content moderation, but it is reasonable to assume that this is the most cost-effective approach and it allows Facebook to wash their hands of the ugly business of content moderation.

Dr. Hany Farid
Page 4

The Honorable Lisa Blunt Rochester (D-DE)

1. **What can the federal government do to improve the capacity and ability to effectively moderate online content, including technological research?**

Response: As we discussed at the hearing, modest changes to Section 230 would go a long way to forcing the technology sector to invest in more effective technological and human moderation. Despite years of public outcry and bad press, profits at Google and Facebook are up. Change will only happen when these companies are held financially responsible for their failure to create safe products that don't lead to the disruption of our democratic elections, don't lead to horrific violence against our citizens, don't lead to allowing child predators to freely exploit children, and don't lead to the daily abuse and marginalization of women and under-represented groups. Like every other industry, the technology sector should be held responsible when their products are unsafe and lead to real and measurable harm.

The Honorable Tom O'Halleran (D-AZ)

1. **Dr. Farid, in the testimony of Dr. McSherry on behalf of the Electronic Frontier Foundation, she states how changes to Section 230 could increase liability risks for platforms and force some to over-censor due to a lack of resources to review content. Dr. McSherry used Craigslist's decision to remove its personal ads section as an example.**
 - a. **With the increasing amount of user-generated content being published on platforms daily, what do you believe to be the correct balance between using algorithms and human reviewers for platforms moderating content?**

Response: I was part of the team that in 2008 developed photoDNA, a technology designed to find, remove, and report child sexual abuse material. At the time we heard from the EFF and others that deployment of this technology would lead to the over moderation of other content. This slippery slope argument is constantly trotted out anytime there is a discussion of content moderation. I find this argument lazy and not backed by the evidence: photoDNA did not, as predicted, lead to over removal of material.

Today, automatic removal of *re-uploaded* content is highly efficient and effective once content has been identified by human moderators as being illegal or a violation of terms of service. Human moderators, however, still need to make the initial determination of what material should be removed. Moving forward, new technologies can and should be developed to automatically flag problematic content, thus reducing the burden on human moderators. I do not, however, foresee the ability to completely remove human moderation in the coming years.

Dr. Hany Farid
Page 5

The Honorable Greg Walden (R-OR)

1. In a letter submitted for the record by TechFreedom, the author states,

“[the Republican staff memo] then claims that “platforms” have failed to meet their end of the bargain: “Internet platforms have, in many instances, benefitted from the ‘shield’ without using the ‘sword’ as intended.” Both claims are false: the first misrepresents the legislative history of Section 230 and the second fails to acknowledge how much interactive computer service providers, both large and small, wield the ‘sword’ of content moderation—and why they do so, without a legal mandate to.

Is the author of that letter correct: have interactive computer service providers met their end of the bargain?

Response: I do not believe they have. From the earliest days of the modern web, the technology giants have followed a similar pattern when it comes to dealing with everything from child sexual abuse material, terrorism and extremism, dangerous and deadly conspiracy theories, dis- and mis-information campaigns, and the sale and distribution of deadly drugs, weapons, and the illegal animal trade: Deny the problem exists, minimize the extent of the problem, concede that the problem is real but deny that a solution is possible, and once there is sufficient public or regulatory pressure, respond as anemically as possible.

Nearly everyone agrees that the technology sector is not doing enough to reign in the abuses and misuses on their services, including web inventor Tim Berners-Lee (see, Mr. Berners-Lee’s *New York Times* op-ed “I Invented the World Wide Web. Here’s How We Can Fix It.” Published on November 24, 2019). The technology sector has consistently put growth and profit over all else and has consistently hid behind Section 230 when called out on their failures.

2. In an October 15, 2019 letter to the Energy and Commerce Committee, TechFreedom states, “The [Republican staff] memo appears to suggest that the shift towards an ‘advertising-centric business models [sic] built upon user-generated content’ has made websites less willing to wield the sword of content moderation. In fact, just the opposite is true: relying on advertising generally gives platforms more of an incentive to monitor and remove objectionable user content.”

That may be true for monitoring and removing objectionable content placed next to ads, but is that the case for affiliated products or platforms that are not as proximate to ads?

Response: The data simply does not support TechFreedom’s argument that an advertising-based economy encourages removal of harmful or illegal material. In fact, all evidence is to the contrary. YouTube, for example, has for years allowed child predators to linger on their services with impunity. It wasn’t until more than three separate Disney-led advertising boycotts, spanning

Dr. Hany Farid

Page 6

several years, that YouTube responded (although with only a limited effort) to reduce the exposure of children to predators and inappropriate content. Facebook has publicly (and almost proudly) claimed that they will allow anyone to explicitly lie in political ads and target advertise these lies with laser focus. Twitter has for years been unable or unwilling to reign in daily abuse, often directed at women and under-represented groups. And, for years, Google has repeatedly failed to remove illegal and dangerous content from their search engine.

The simple fact is that when services like Google/YouTube, Facebook, and Twitter are free, these companies are not answerable to us the public. They need only appease the advertisers which in turn need only see – with few exceptions – a return on their advertising dollars. The advertising driven technology sector – once thought to be a boom for the public – is the underlying poison of the today's internet. This business model puts engagement, views, likes, and shares, ahead of all else.

