S. HRG. 118–33

PLATFORM ACCOUNTABILITY: GONZALEZ AND REFORM

HEARING

BEFORE THE

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MARCH 8, 2023

Serial No. J–118–7

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PUBLISHING OFFICE
52–654 PDF WASHINGTON : 2023

COMMITTEE ON THE JUDICIARY

RICHARD J. DURBIN, Illinois, *Chair*

DIANNE FEINSTEIN, California
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
CHRISTOPHER A. COONS, Delaware
RICHARD BLUMENTHAL, Connecticut
MAZIE K. HIRONO, Hawaii
CORY A. BOOKER, New Jersey
ALEX PADILLA, California
JON OSSOFF, Georgia
PETER WELCH, Vermont

LINDSEY O. GRAHAM, South Carolina, *Ranking Member*
CHARLES E. GRASSLEY, Iowa
JOHN CORNYN, Texas
MICHAEL S. LEE, Utah
TED CRUZ, Texas
JOSH HAWLEY, Missouri
TOM COTTON, Arkansas
JOHN KENNEDY, Louisiana
THOM TILLIS, North Carolina
MARSHA BLACKBURN, Tennessee

JOSEPH ZOGBY, *Chief Counsel and Staff Director*
KATHERINE NIKAS, *Republican Chief Counsel and Staff Director*

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW

RICHARD BLUMENTHAL, Connecticut, *Chair*

AMY KLOBUCHAR, Minnesota
CHRISTOPHER A. COONS, Delaware
MAZIE K. HIRONO, Hawaii
ALEX PADILLA, California
JON OSSOFF, Georgia

JOSH HAWLEY, Missouri, *Ranking Member*
JOHN KENNEDY, Louisiana
MARSHA BLACKBURN, Tennessee
MICHAEL S. LEE, Utah
JOHN CORNYN, Texas

DAVID STOOPLER, *Democratic Chief Counsel*
MICHAEL VELCHIK, *Republican Chief Counsel*

CONTENTS

MARCH 8, 2023, 2:05 P.M.

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS

ANSWERS

MISCELLANEOUS SUBMISSIONS FOR THE RECORD

Submitted by Chair Blumenthal:

PLATFORM ACCOUNTABILITY: GONZALEZ AND REFORM

WEDNESDAY, MARCH 8, 2023

UNITED STATES SENATE,
SUBCOMMITTEE ON PRIVACY, TECHNOLOGY,
AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice at 2:05 p.m., in Room 226, Dirksen Senate Office Building, Hon. Richard Blumenthal, Chair of the Subcommittee, presiding.

Present: Senators Blumenthal [presiding], Klobuchar, Hirono, Padilla, Hawley, and Blackburn.

Also present: Chair Durbin.

OPENING STATEMENT OF HON. RICHARD BLUMENTHAL, A U.S. SENATOR FROM THE STATE OF CONNECTICUT

Chair BLUMENTHAL. The Senate Subcommittee on Privacy, Technology, and Law is convened. We are a Subcommittee of the Judiciary Committee and the Chairman of our Committee is with us today. I want to thank all of our panel for being here, all of the members of the audience who are attending, and my Ranking Member, colleague, partner in this effort, Senator Hawley. I'm going to turn first to the Chairman because he has an obligation on the floor for some opening remarks. We're very pleased that he's with us today.

OPENING STATEMENT OF HON. RICHARD J. DURBIN, A U.S. SENATOR FROM THE STATE OF ILLINOIS

Chair DURBIN. Senator Blumenthal and Senator Hawley, thank you for holding this important meeting. We had a rather historic meeting of the Senate Judiciary Committee just a few weeks ago. I think everybody agreed on subject matter of the hearing. I don't know when that's ever happened, at least recently. And it was encouraging.

The hearing considered the subject of protecting kids online. One of the witnesses we heard from, Kristin Bride, a mother with a son who died by suicide after he was mercilessly bullied on an anonymous messaging app. There were several other mothers in attendance carrying color photos of their kids who suffered similar heartbreak.

In addition to tragically losing children, these mothers had something else in common. They couldn't hold the online platform that

played a role in their child's death accountable. The reason, Section 230, well known to everyone who's taken a look at this industry.

Coincidentally, after that hearing, I had a meeting with the administrator of the Drug Enforcement Administration, Anne Milgram. She described for me how illegal and counterfeit drugs are sold over the internet to kids, often with devastating results. When I asked her what online platforms were doing to stop it, she said very little, and refusing to cooperate with her agency to even investigate.

I asked her, "How do they deliver these drugs? By mail?" Oh, no. By valet service. They bring boxes of these counterfeit drugs, deadly drugs, leave them on the front porch of the homes of these kids. Imagine this, we're talking about a medium that is facilitating that to occur in America. These platforms know these drug transactions are happening. What are they doing about them? Almost nothing. Why? Section 230.

In our hearing last month, there seemed to be a consensus emerging, Democrats and Republicans, that we've got to do something to make Section 230 make sense. Something needs to change so online platforms have an incentive to protect children, and if they don't, they should be held liable in civil actions.

I look forward to hearing from the witnesses today. I'm sorry I can't stay because I have major on the floor to consider in a few minutes, but I will review your testimony, and thank you for your input. Thank you, Mr. Chairman, Ranking Member.

Chair BLUMENTHAL. Thanks very much, Senator Durbin. I think it is a mark of the importance and the imminence of reform that Senator Durbin is here today. His leadership led to the hearing that we had just a couple weeks ago, showing the harms, really desperate, despicable harms that can result from some of the content on the internet and the need to hold accountable the people who put it there. And that's very simply why we are here today.

I want to thank Senator Durbin for his leadership. Also, Senator Coons who preceded me as head of this Subcommittee. There are certainly challenging issues before us on this Subcommittee from reining in Big Tech to protecting our civil rights in an era of artificial intelligence.

And I am enormously encouraged and energized by the fact that we have bipartisan consensus on this first hearing. Not always the case in the Judiciary Committee, not always the case in the United States Senate, but I'm really appreciative of Senator Hawley's role, especially his amicus brief to the United States Supreme Court in *Gonzalez*.

The comments by the Solicitor General in that case, some of the comments by the Justices, we have no ruling yet, but I think what we are seeing is, as Senator Durbin said, an emerging consensus that something has to be done.

So here's a message to Big Tech, reform is coming. Can't predict it'll be in the next couple weeks or the next couple months, but if you listen, you will hear a mounting consensus and a demand from the American public that we need to act in a bipartisan way.

Section 230 dates from a time when the internet was a young, nascent startup kind of venture that needed protection if it tried to weed out the bad stuff. And now it's used to defend keeping the

bad stuff there. This so-called shield has been long outdated as we enter an era of algorithms and artificial intelligence, which were unknown and perhaps unimaginable on the scale that they now operate when Section 230 was adopted.

And the caselaw—and I've read it, the *Gonzalez* Court addressed it—simply doesn't provide the kind of remedy that we need quickly enough and thoroughly enough. I think that the time when the internet could be regarded as a kind of neutral or a passive conduit has long since passed. Obviously, we need to look at platform design, the business operations, the personalization of algorithms, recommendations that drive content.

And we've seen it particularly with children. Toxic content driven by algorithms in a very addictive way toward children with this overwhelming protection that is accorded by Section 230 to the tech platforms that are responsible and need to be held accountable.

Section 230 actually was designed to promote a safer internet. Plainly, it's doing the opposite right now. And what we have heard graphically as Senator Durbin described it again and again and again at hearings in the Commerce Committee, the Subcommittee on Consumer Protection, which I chaired, hearing from the whistleblower, Frances Haugen, documents that we've seen from Facebook and the victims and survivors, Mrs. Bride, who lost her son, Carson.

Anastasia, who wrote me along with another young woman, Saanvi Arora and Anastasia Chaglasian, they started a petition that received 30,000 signatures from Americans across the Nation after they were victimized. Pictures of their sexual abuse repeatedly transmitted on anonymous platforms. And I'm going to put their letter to me in the record without objection.

[The information appears as a submission for the record.]

Chair BLUMENTHAL. But the point is, we've seen the harms. We need to take action to address those harms. And we've also seen harms, Section 230 has shielded platforms like Craigslist when they hosted housing ads that openly proclaimed no minorities. Section 230 has immunized Facebook when its own advertising tools empowered and encouraged landlords to exclude racial minorities and people with disabilities. For any other company, these would be violations of the Fair Housing Act, but Section 230 shut the door on accountability for them and in so many other instances.

The case history on Section 230 is clear. When Big Tech firms invoke it, those being denied justice are often women, people of color, members of the LGBTQ community or children, and the victims and survivors of sexual abuse. So this hearing is very simply part of a broader effort to reform Section 230.

We've seen some of the models and the frameworks that are possible for reform. I'm not taking sides right now, but by the end of these hearings, I hope to do so, and this enterprise is not new for me. Fifteen years ago when I was Attorney General dealing with Myspace and Craigslist and many of the same issues that we're confronting today, I said to my staff, "We should repeal Section 230." And they came down on me like a house of bricks and said, "Whoa, you can't repeal Section 230. That's the Bible of the internet."

Well, it's not the Bible of the internet. It's not the 10 Commandments that have been handed down. It is a construct that is now outdated and outmoded and needs reform. And I'm really so thankful to have the leadership of Senator Hawley, who is also a longstanding champion of survivors and victims of sexual abuse and other harms. And to his great credit, a former State attorney general. Senator Hawley.

OPENING STATEMENT OF HON. JOSH HAWLEY, A U.S. SENATOR FROM THE STATE OF MISSOURI

Senator HAWLEY. Thank you very much, Senator Blumenthal. Thank you, Mr. Chairman, for being here as well. Thanks to all the witnesses for making, in some cases, the long trek here. I just want to add a few remarks. I am delighted that the first meeting of this Subcommittee is focusing on what is, I think, maybe the critical issue in this space, and that is Section 230.

And I want to amplify something that Senator Blumenthal just said, which is that Section 230, as we know it today, is not only outmoded, it's not only outdated, it's really completely unrecognizable from what Congress wrote in the 1990s. I mean, let's be honest, the Supreme Court heard arguments to this effect just a few weeks ago, but the Section 230, as we know it today, has been almost completely rewritten by courts and other advocates, usually at the behest of Big Tech, the biggest, most powerful corporations, not just now, but in the history of this country.

They have systematically rewritten Section 230. And listen, I hope that the United States Supreme Court will do something about it because frankly, they share some of the blame for this. And I hope in the *Gonzalez* case, they'll begin to remedy that. But whatever the case may be there, it is incumbent upon Congress to act. We wrote Section 230 originally. We should fix it now. And I welcome these hearings to collect evidence, to hear from experts such as those who are before us today about the paths forward.

From my own view, I think that some of the common ground that Senator Blumenthal mentioned and that the Chairman mentioned that we've heard in our hearings recently really boils down to this: It really is time to give victims their day in court. What could be more American than that? Every American should have the right, when they have been injured, to get into court, to present their case, to be heard, and to try to be made whole.

Section 230 has prevented that for too many years. And I would hope that if we could agree on nothing else, we could agree on that basic, fundamental, dare I say, fundamentally American approach. And I hope that that's something that we'll be able to explore together.

Now, I just note that progress on reforming Section 230 has been very slow. As a Republican, I would love to blame that on my Democrat colleagues, but the sad fact of the matter is Republicans are just as much to blame, if not more. And my own side of the aisle when it comes to vindicating the rights of citizens to get into court, to have their day in court, has often been very, very slow to endorse that approach and very, very wary.

But I think that the time has come to say that we must give individuals, we must give parents, we must give kids and victims

that most basic right. And I hope that this Subcommittee and the Committee as a whole, the Judiciary Committee as a whole, will prove in this Congress that real bipartisan action with real teeth is possible. And we will see real reform for America's families and children. Thank you, Mr. Chairman.

Chair BLUMENTHAL. Thanks, Senator Hawley. I'm going to introduce the panel. And then, as is our custom, I will swear you in and ask you for your opening remarks.

Dr. Mary Anne Franks is an internationally recognized expert on the intersection of civil rights and technology. She's a professor of law and the Michael Klein Distinguished Scholar Chair at the University of Miami, and the president and legislative and tech policy director of this Cyber Civil Rights Initiative, a nonprofit organization dedicated to combating online abuse and discrimination.

Professor Hany Farid is a professor of computer science at UC, Berkeley. He specializes in image and video analysis and developing technologies to mitigate online harms, ranging from child sexual abuse to terrorism and deepfakes.

Ms. Jennifer Bennett is a principal at Gupta Wessler, where she focuses on appellate and Supreme Court advocacy on behalf of workers, consumers, and civil rights plaintiffs. She recently argued and won *Henderson v. Public Data*, a Section 230 appeal before the Fourth Circuit that established a framework for interpreting the statute that has for the first time garnered widespread support.

Andrew Sullivan is the president and CEO of the Internet Society, a global nonprofit organization founded to build, promote, and defend the internet. Mr. Sullivan has decades of experience in the internet industry having worked to enhance the internet's value as an open global platform throughout his career.

Finally, Professor Eric Schnapper is professor of law at the University of Washington School of Law in Seattle. He recently argued the cases of *Gonzalez v. Google* and *Twitter v. Taamneh* before the United States Supreme Court. Before joining the University of Washington faculty, he spent 25 years as an assistant counsel for the NAACP Legal Defense and Educational Fund in New York City, and he also worked for Congressman Tom Lantos. He is a member of the Washington Advisory Committee of the United States Commission on Civil Rights. I assume that your appearance today will not be as arduous as arguing two Supreme Court cases back to back.

Would the witnesses please stand and raise your right hand?

[Witnesses are sworn in.]

Chair BLUMENTHAL. Thank you.

Senator WHITEHOUSE. Mr. Chairman, does this mean that for the first time you're not the person in the room who's argued the most Supreme Court decisions?

Chair BLUMENTHAL. Well, I've done four, but I think Mr. Schnapper may exceed my record in total. I'm not sure. Let's begin with Dr. Franks.

STATEMENT OF MARY ANNE FRANKS, PROFESSOR OF LAW AND THE MICHAEL R. KLEIN DISTINGUISHED SCHOLAR CHAIR, UNIVERSITY OF MIAMI SCHOOL OF LAW, MIAMI, FLORIDA

Professor FRANKS. Thank you. In 2019, nude photos and videos of an alleged rape victim were posted on Facebook by the man accused of raping her. The posting of non-consensual intimate imagery is prohibited by Facebook's terms of service. The company's operational guidelines stipulate that such imagery should be removed immediately and that the account of the user who has posted it should be deleted.

However, Facebook moderators were blocked from removing the imagery for more than 24 hours, which allowed the material—which the company itself described in internal documents as revenge porn—to be reposted 6,000 times and viewed by 56 million Facebook and Instagram users leading to abuse and harassment of the woman.

The reason why, according to internal documents obtained by the Wall Street Journal, was that the man who had posted the non-consensual pornography was a famous soccer star. That is, this was no mere oversight, but rather an intentional decision by the company to make an exception for an elite user. This was in accordance with a secret Facebook policy known as cross-check, which grants politicians, celebrities, and popular athletes special treatment for violation of platform rules.

The public only knows about this policy because of whistleblowers and journalists who also revealed Meta's full knowledge of Facebook's role in genocide and other violence in developing countries, the harmful health effects of Facebook and Instagram use on young users, and the corrosive and anti-democratic impact of misinformation and disinformation amplified through its platforms.

The law that is currently interpreted to allow Facebook and other tech platforms to knowingly profit from harmful content was passed by Congress in 1996 as a Good Samaritan law for the internet. Good Samaritan laws provide immunity from civil liability to incentivize people to help when they are not legally obligated to do so.

The title of the operative provision of this law and the text of Section 230(c)(2) reflect the 1996 House Committee reports description of the law as providing, quote, "Good Samaritan protections from civil liability for providers or users of an interactive computer service for actions to restrict or to enable the restriction of access to objectionable online material."

How did a law that was intended as a shield for platforms who restrict harmful content become a sword for platforms that promote harmful content? By ignoring the legislative purpose, history, and the statute's language as a whole to focus on a single sentence that reads, "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."

The use of the words publisher or speaker, which are terms of art from defamation law, make clear that this provision bars certain types of defamation and defamation-like claims that attempt

to impose liability on people simply for repeating or providing access to unlawful content.

But many courts have instead interpreted this sentence to grant unqualified immunity to platforms against virtually all claims and for virtually all content. An interpretation that not only destroys any incentive for platforms to voluntarily restrict content, but in fact provides them with every incentive to encourage and amplify it.

The Supreme Court, in taking up *Gonzalez v. Google*, has the opportunity to undo more than 20 years of the preferential and deferential treatment of the tech industry that has resulted from the textually unsupported and unintelligible reading of the statute. It was an encouraging sign during oral argument that many Justices pushed back against the conflation of a lack of community with the imposition of liability and seemed unconvinced by claims that the loss of preemptive, unqualified immunity would destroy the tech industry.

As Justice Kagan observed, "Every other industry has to internalize the costs of its conduct. Why is it that the tech industry gets a pass?" Supporters of the Section 230 status quo respond that the tech industry is special because it is a speech-focused industry. This claim is disingenuous for two reasons.

First, Section 230 is invoked as a defense for a wide range of conduct, not only speech. And second, other speech-focused industries do not enjoy the supercharged immunity that the tech industry claims is essential for its functioning.

Colleges and universities are very much in the business of speech, but they can be sued. As can book publishers and book distributors, radio stations, newspapers, and television companies. Indeed, The New York Times and Fox News have both recently been subjected to high-profile defamation lawsuits.

The newspaper and television industries have not collapsed under the weight of potential liability, nor can it be plausibly claimed that the potential for liability has constrained them to publish and broadcast only anodyne, non-controversial speech.

There's no guarantee that the Supreme Court will address the Section 230 problem directly or in a way that would meaningfully restrict its unjustifiably broad expansion. And so, Congress should not hesitate to take up the responsibility of amending Section 230 to clarify its purpose and foreclose interpretations that render the statute internally incoherent and allow the tech industry to inflict harm with impunity.

At a minimum, this would require amending the statute to make clear that the law's protections only apply to speech, and to make clear that platforms that knowingly promote harmful content are ineligible for immunity. Thank you.

[The prepared statement of Professor Franks appears as a submission for the record.]

Chair BLUMENTHAL. Thank you. Thank you very much, Dr. Franks. Professor Farid.

STATEMENT OF HANY FARID, PROFESSOR, SCHOOL OF INFORMATION AND ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, UNIVERSITY OF CALIFORNIA, BERKLEY, BERKELEY, CALIFORNIA

Professor FARID. Chair Blumenthal, Ranking Member Hawley, and Members of the Subcommittee, thank you. In the summer of 2017, three Wisconsin teenagers were killed in a high-speed car crash. At the time of the crash, the boys were recording their speed of 123 miles an hour on Snapchat's speed filter.

Following the strategy, the parents of the passengers sued Snapchat claiming that the product which awarded trophies, streaks, and social recognition was negligently designed to encourage dangerous high-speed driving. In 2021, the Ninth Circuit ruled in favor of the parents and reversed a lower court's ruling that had previously emphasized that the speed filter as creating third-party content, thus finding that Snapchat was not deserving of 230 protection.

Section 230, of course, immunizes platforms and that they cannot be treated as a publisher or speaker of third-party content. In this case, however, the Ninth Circuit found the plaintiff's claims did not seek to hold Snapchat liable for content, but rather for a faulty product design that predictably encouraged dangerous behavior. This landmark case, *Lemmon v. Snap*, made a critical distinction between a product's negligent design and the underlying user-generated content, and this is going to be the theme of my opening statements here.

Frustratingly, over the past several years, most of the discussion of 230, and most recently in *Gonzalez v. Google*, this fundamental distinction between design and content has been overlooked and muddled. At the heart of *Gonzalez* is whether 230 immunizes YouTube when they not only host third-party content, but make targeted recommendations of content.

Google's attorneys argued that fundamental to organizing the world's information is the need to algorithmically sort and prioritize content. In this argument, however, they conveniently conflate a search feature with a recommendation feature. In the former, the algorithmic order of content is critical to the function of a Google or a Bing search.

In the latter, however, YouTube's "watch next" and "recommended for you" features, which lie at the core of *Gonzalez*, are a fundamental design decision that materially contributes to the product safety. The core functionality of YouTube as a video-sharing site is to allow users to upload a video, allow other users to view the video, and possibly search videos.

The basic functionality of recommending content—of which 70 percent of watched videos on YouTube are recommended—is done in order to increase user engagement and, in turn, ad revenue. It is not a core functionality. YouTube has argued that the recommendation algorithms are neutral and that they operate the same way as it pertains to a cat or an ISIS video. This means then that because YouTube can't distinguish between a cat and an ISIS video, they've negligently designed their recommendation engine.

YouTube has also argued that with 500 hours of video uploaded every minute, they must make decisions on how to organize this

massive amount of content. But again, searching for a video based on a creator or a topic is distinct from YouTube's design of a recommendation feature whose sole purpose is to increase YouTube's profits by encouraging users to binge-watch more videos.

In so doing, the recommendation feature prioritizes increasingly more bizarre and dangerous rabbit holes full of extremism, conspiracies, and dubious alternate facts. Similar to Snapchat's design, a decision to create a speed filter, YouTube chose to create this recommendation feature, and they either knew or should have known that it was leading to harm.

By focusing on 230 immunity from user-generated content, we are overlooking product design decisions, which predictively have allowed and even encouraged terror groups like ISIS to use YouTube to radicalize, recruit, and glorify global terror attacks.

While much of the debate around 230 has been highly partisan—on this, Senator Hawley, we agree—it need not be. The core issue is not one of over or under moderation, but rather one of a faulty and an unsafe product design. As we routinely do in the offline world, we can insist that the technology in our pockets are safe.

So, for example, we've done a really good job of making sure that the battery powering our device doesn't explode and kill us, but we've been negligent in ensuring that the software running on device is safe. The core tenets of 230, limited liability for hosting user-generated content, can be protected while insisting, as in *Lemmon v. Snap*, the technology that is now an inextricable part of our lives be designed in a way that is safe.

This can be accomplished by clarifying that 230 is intended to protect platforms from liability based exclusively on their hosting of user-generated content and not as has been expanded to include a platform's design features that we now know is leading to many of the harms that Senator Blumenthal opened with at the very beginning. Thank you.

[The prepared statement of Professor Farid appears as a submission for the record.]

Chair BLUMENTHAL. Thank you very much, Professor. Ms. Bennett.

STATEMENT OF MS. JENNIFER BENNETT, PRINCIPAL, GUPTA WESSLER PLLC, SAN FRANCISCO, CALIFORNIA

Ms. BENNETT. Good afternoon. Thank you for the opportunity to testify before you today. I'm going to focus on, Senator Blumenthal mentioned this case, *Henderson v. Public Data*, and I'm going to focus on that case. And the reason for focusing on that case is because if you look at the transcript in *Gonzalez* of the oral argument, what you'll see is that the parties there disagreed about virtually everything, the facts, the law, whether the sky is blue and the grass is green, everything.

The one thing, the one place they found common ground was that this case, *Henderson*, got Section 230 right. And so in thinking about what Section 230 means, what it means, how it might be reformed, I think *Henderson* might be a good starting place. So what is this magical framework that gets Google and the people suing Google and the United States Government all on the same page?

This framework has two parts, and it mirrors the two parts of 230 that people typically fight about. So part 1 addresses what does it mean to treat someone as a publisher? Because Section 230 says, "We'll protect you from claims that treat you as a publisher of third-party content." But it doesn't say what that means.

And what *Henderson* says is, "Well, we know that publisher liability, what Section 230 is saying about publisher liability comes from defamation law." And in defamation law, what publisher liability means is holding someone liable for disseminating to third parties' content that's improper.

So, for example, someone goes on Facebook, they say, "Jennifer Bennett is a murderer." I am not in fact a murderer, so I sue Facebook for defamation. That claim treats Facebook as a publisher. Because what it's saying is, "Facebook, you're liable because you've disseminated to third parties information that I think is improper."

On the other hand, say I apply for a job and the employer wants to find out some things about me so they go online and they buy a background check report about me, and the online background check company doesn't see if the employer got my consent. And so, I sue that company. I say the Fair Credit Reporting Act requires you to ask the employer if they have consent. You didn't do that.

That claim, as *Henderson* holds, doesn't treat the company as a publisher. And the reason for that is that the claim doesn't depend on anything improper about the content. The claim says, "You, company, were supposed to do something and you didn't do it." It's a claim based on the conduct of the company, not on content.

So that's part 1 of the *Henderson* framework. A claim only treats someone as a publisher if it imposes liability for disseminating information to third parties, where the claim is that information is improper for some reason.

Part 2 of the *Henderson* framework is what it means to be responsible for content. Because even if a claim treats someone as a publisher, Section 230 as written, offers no protection if they're responsible, even in part for the creation or the development of that content.

And what *Henderson* says, and this is what a lot of courts have said actually, is that at the very least, if you materially contribute to what makes the content unlawful, then you're responsible and Section 230 should offer no protection to you.

So to take a seminal example, say there's a housing website, and to post a listing on the housing website, the website requires you to pick certain races of people to which you'll offer housing. And so, there's a listing that says whites only. Someone sues the website and says, you're discriminating. It violates the Fair Housing Act.

The website should have no protection in that case because the website materially contributed to what's unlawful about the posting. The website said you have to pick races of people who the listing should be available to. So that's part 2 of the *Henderson* framework, which is you're responsible for conduct, content rather, and you're outside the protection of Section 230, even as it currently exists, if you created that content or materially contributed to what's unlawful about it.

And I just want to end by noting that both parts of this framework depend on the same fundamental premise. And I think that's what's driving people's, you know, even Google's willingness to say this case is correct.

And that fundamental premise is that Section 230 protects internet companies and internet users from liability when the claim is based solely on improper content that someone else chose to put on the internet, but it doesn't protect, and what it was never intended to protect, is to protect platforms from liability based on their own actions. Thank you, again. I look forward to any questions.

[The prepared statement of Ms. Bennett appears as a submission for the record.]

Chair BLUMENTHAL. Thank you very much, Ms. Bennett. Mr. Sullivan.

STATEMENT OF MR. ANDREW SULLIVAN, PRESIDENT AND CHIEF EXECUTIVE OFFICER, INTERNET SOCIETY, RESTON, VIRGINIA

Mr. SULLIVAN. Good afternoon, Chair Blumenthal, Ranking Member Hawley, and distinguished Members of this Subcommittee. Thank you for this opportunity to appear before you today to discuss platform accountability.

I work for the Internet Society. We are a U.S. incorporated public charity founded in 1992. Some of our founders were part of the very invention of the internet. We have headquarters in Reston, Virginia, and in Geneva. Our goal is to make sure that the internet is for everyone. Making sure that is possible is what brings me here before you today.

The internet is in part astonishing because it is about people. Many communications technologies either allow individuals only to speak to one another, or they allow one central source, often corporate-controlled, to address large numbers of people at one time. The internet, by contrast, allows everyone to speak to anyone. That can sometimes be a problem. I too am distressed by the serious harms that come through the internet and that we have heard about today.

But I also know the benefits that the internet brings, whether that be for isolated people in crisis who find the health that they need online, or to those who learn a new useful skill through freely shared resources, or to still others who are led to new insights or devotions through their interactions with others. People interact with one another on the internet and Congress noted this important feature in Section 230 with its emphasis on how the internet is an interactive computer service.

Yet the internet is a peculiar technology because it is not really a single system. Instead, it is made up of many separate participating systems, all operating independently. The independent participants, including ordinary people just using the internet, all use common technical building blocks without any central control. And when we put all these different systems together, we get the internet.

Section 230 emerged just as the internet was ceasing to be a research project and turning into the important communication medium it is today. But even though Congress was facing something

strange and new, the legislators understood these two central features. The interactive nature meant that people could share in ways other technologies hadn't enabled. And the sheer number of participants meant that each of them needed to be protected from liability for things that other people said. The internet has thrived as a result. And this is what concerns me about proposals either to repeal Section 230 or to modify it substantially.

Outright repeal would be a calamity as online speech would quickly be restricted from fear of liability. Even the trivial things, retweeting a news article, sharing somebody else's restaurant review would incur too great a risk that somebody would say something and make you liable. So anyone operating anything on the internet would rationally restrict such behaviors.

Even something narrowly aimed at the largest corporate players presents a risk to the internet. In a highly distributed system like this, you can try something without anyone else being involved, but if some players have special rules, it is important that everyone else not be subject to those rules by accident, because those others don't have the financial resources of the special players.

It would be bad to create a rule that only the richest companies could afford to meet. It would give them a permanent advantage over potential new competitors. Issues of the sort Americans are justly worried about naturally inspire a response. It is entirely welcome for this Subcommittee to be examining these issues today.

But because Section 230 protects the entire internet, including the variability of individuals to participate in it, it is a poor vehicle to address admittedly grave and insidious problems that are nevertheless caused by a small subset of those online. This is not to say that Congress is powerless to address these important social problems.

Approaches that give rights to all Americans, such as baseline privacy legislation, could start to address some of the current lack of protections in the online sphere. Given the concerns about platform size, competition policy is another obvious avenue to explore.

We at the Internet Society stand ever willing to consult and provide feedback on any proposals to address social problems online. I thank you for the opportunity to speak to you today. I look forward to answering any questions you have, and of course, we would be delighted to engage with any of your staff on specific proposals. Thank you.

[The prepared statement of Mr. Sullivan appears as a submission for the record.]

Chair BLUMENTHAL. Thanks, Mr. Sullivan.

Professor Schnapper.

STATEMENT OF ERIC SCHNAPPER, PROFESSOR OF LAW, UNIVERSITY OF WASHINGTON SCHOOL OF LAW, SEATTLE, WASHINGTON

Professor SCHNAPPER. Thank you. Senator Durbin and——

Chair BLUMENTHAL. You might turn on your microphone.

Professor SCHNAPPER. Senator Durbin and yourself, Senator Blumenthal, you put your finger on the core problem here, which is that Section 230 has removed the fundamental incentive that the legal system ought to provide to avoid doing harm. And the con-

sequence of that statute has been precisely as Senator Hawley described, that the right of Americans to obtain redress if they've been harmed by knowing misconduct has been eviscerated.

Now, part of the concern that led to the adoption of the statute was that internet companies wouldn't know what was on their websites, but there's—we have decades of experience with the fact that they know exactly what's going on and they don't do anything about it. And the presence of terrorist materials on their websites, and the fact that those materials are being recommended has long been known.

Federal officials have been raising this with the internet companies for 18 years. In 2005, Senator Lieberman, whom you know well, wrote a letter to these companies and asked them to do something about terrorist materials on their websites.

Since then, Members of the other body and of the administration have made that point publicly. There have been dozens of published articles about the use of the websites by terrorist organizations. I brought a sample today, a small fraction. I mean, I'm happy to provide the staff with other examples.

Chair BLUMENTHAL. We'll ask that those materials be entered in the record without objection.

[The information appears as submissions for the record.]

Professor SCHNAPPER. You may want to see how many there are before you put them all on the record.

[Laughter.]

Chair BLUMENTHAL. We have a big record.

Professor SCHNAPPER. The terrorist attacks were so rooted in what was going on in the internet that when there was a rash of terrorist attacks in the state of Israel, they were known as the Facebook intifada. And complaints were made to the social media companies without effect.

In January 2015, the problem was so serious that there was a meeting with internet executives in which the representatives of the Federal Government were the Attorney General, the Director of the FBI, the Director of National Intelligence, and the White House Chief of Staff and I urge the Committee to ask for a readout of that meeting and what those companies were told.

Most recently, in the *Twitter* litigation, a group of retired generals filed a brief describing the critical role that social media had played in the rise of ISIS. And again, I commend that brief to you. I think it's extremely informative of their informed military judgment about the consequences of what's been happening.

The response of social media to this problem has often been indifferent and sometimes deeply irresponsible. In August and September 2014, two American journalists were murdered by ISIS. They were brutally beheaded and the killings were videotaped.

When Twitter was called upon to stop publicizing those types of events, an official commented, "One man's terrorist is another man's freedom fighter." That illustrates how fundamentally wrong the status of the law is today. And there's a good account of other comments like that from social media in a brief that was filed by the Concerned Women for America, which describes efforts and responses of that kind.

What we have learned from the past 25 years is that absolute immunity can breed absolute irresponsibility. Now, we understand that private corporations exist to make a profit, but they also have obligations to the rest of the country and to your constituents to be concerned about the harms they can cause. Google and Meta have made billions of dollars since the enactment of Section 230, and Twitter may yet turn a profit. But those firms have a long way to go before they emerge from moral bankruptcy. Thank you.

[The prepared statement of Professor Schnapper appears as a submission for the record.]

Chair BLUMENTHAL. Thank you, Professor Schnapper. You argued before the United States Supreme Court. I think it's pretty fair to say that the Court was struggling with many of these issues. And Justice Kagan said, quote, "Every other industry has to internalize the costs of misconduct. Why is it that the tech industry gets a pass? A little bit unclear," end quote.

She went on to say, "On the other hand, I mean, we're a court. We really don't know about these things. You know, we are not like the greatest experts on the internet." That became clear, I think, in the course of the argument, but it also emphasizes the importance of what we're doing here. Because, ultimately, my guess is that the Court will turn to Congress.

But I think it's also worth citing a remark by Chief Justice Roberts when he said, "The videos," I'm quoting, "just don't appear out of thin air. They appear pursuant to the algorithms," end quote. The Supreme Court understands that these videos, the content very often is driven, it's recommended, it's promoted, it's lifted up, sometimes in a very addictive way to kids. And some of it absolutely abhorrent, to which they have been, as you put it Professor Schnapper, indifferent or downright irresponsible.

And let me just make clear, Mr. Sullivan, we are not denying the benefits of the internet that—important benefits in interactive communication and the large number of participants. But the cases that have begun to make a start toward reining in Section 230: *Henderson*, described by Ms. Bennett, but before it, *Roommates* and *Lemmon*, both cases that try to do carve-outs in a way, *Henderson*, based on the material contribution case, show that we can establish limits without breaking the internet and without denying those benefits.

Let me ask you, Ms. Franks, you know well, the material contribution test. In your testimony, you distinguish—you make another potential distinction or test involving information versus speech. I wonder if you could comment on the material contribution test, whether it is sufficient or whether we need a different kind of standard incorporated into the statute.

Professor FRANKS. Thank you. As to the first question, I think the material contribution test would be useful if we had agreement about what it meant. And there seems to be a lot of uncertainty about how to apply that test. And so, I would be concerned that that test would be difficult to codify. What I think on the other hand would be—a promising approach would be to incorporate some standard along the lines of deliberate indifference to unlawful content or conduct.

And to relate to the other part of your question, the reason why I've advocated for a specific amendment that would change the word "information" to "speech" is partly because a lot of the rhetoric that surrounds much of the defense of the status quo is that it's intended to defend free speech in some sort of general sense.

That the tech industry is able to leverage that halo of the First Amendment to say, "If it weren't for us, you wouldn't get to have any free speech." And I think that is suspect for many reasons, not least because the kind of speech that is often encouraged by these platforms and amplified is speech that silences and chills vulnerable groups.

But it is also troubling because a lot of what gets invoked for Section 230's protections are not speech, or at least are not uncontroversially speech. And what I mean by this is that the Supreme Court has actually had to struggle over decades to figure out whether or not, for instance, an armband is speech or whether the displays of certain flags are speech. And, ultimately, the Supreme Court has been quite protective of certain types of conduct that they deem to be expressive.

But usually, that takes some sort of explicit consideration and reflection as to, is this expressive enough conduct to get the benefit of First Amendment protection? And by putting the word information and allowing that to be interpreted incredibly widely, what companies are able to do is to short-circuit that kind of debate over whether or not what they're actually doing and what they're involved with is in fact speech.

And I think that the clarification that it has to be speech and that the burden should have to be on companies to show that what they are at—what is at issue is in fact speech, I think that would be very helpful.

Chair BLUMENTHAL. Thank you. I have many more questions. I'm going to stay within the 5-minute limit so that as many as possible my colleague can ask their question. And turn now to Senator Hawley.

Senator HAWLEY. Thank you very much, Mr. Chairman. Professor Schnapper, let me start with you. Thinking about the arguments that you made in both the *Gonzalez* case and then also in the *Twitter* case recently, in both of those cases, just to make sure that folks who are listening understand it, you were arguing on behalf of victims' families that were challenging the tech companies. Have I got that basically?

Professor SCHNAPPER. Yes, sir.

Senator HAWLEY. So the Court, of course, is deliberating on this case as we don't know exactly what they're going to do. We'll have to wait to find out. But in both of these cases, help us understand your argument and set the scene for us. You are arguing that there is a difference. These tech companies have moved beyond merely hosting user-generated content to affirmatively recommending and promoting user-generated content. Is that right? Is that——

Professor SCHNAPPER. That's correct.

Senator HAWLEY. So explain to us the significance of that. What's the difference between claiming immunity from not just hosting user-generated content, but now claiming immunity from pro-

moting and affirmatively recommending and pushing user-generated content?

Professor SCHNAPPER. Well, I think that's a distinction that derives from the wording of the statute. The statute seeks to distinguish between conduct of a website itself and materials that were simply created by others. And that distinction's clear on the face of the statute and the legislative history.

Representative Lofgren at one point said, "Holding internet companies responsible for defamatory material would be like holding the mailman," those are the language that we used at the time, "responsible for delivering a plain, brown envelope." What's happening today is a far afield from merely delivering plain, brown envelopes. Internet companies are promoting this material, and they're doing it to make money.

At the end of the day, social media companies make money by selling advertisements. The longer someone is online, the more advertisements they sell. And they have developed an extraordinarily effective and sophisticated system of algorithms to promote material and keep people online. And it sweeps up cat videos and it sweeps up terrorist materials and it sweeps in depictions of tragically underweight young women with dreadful consequences. So that's the distinction we were drawing.

Senator HAWLEY. You mentioned algorithms and I think this is so important. Tell us why you think these algorithms which didn't generate themselves—the algorithms are designed by humans, they're designed by the companies. In fact, the companies regard them as very proprietary information. I mean, they protect them with their lives, the essence of their companies, their business model in many cases.

Tell us what legal difference under Section 230 you think these algorithms and algorithmic promotion makes in these kind of cases. Why is that such a key factor?

Professor SCHNAPPER. Well, the algorithms are the method by which the companies achieve their goal of trying to interest a viewer in a particular video or text or whatever.

And it's done in a variety of ways. It's done with auto-play so that you turn on one video and you start to see a series of others that you never asked for. It's done through little advertisements. They're known as thumbnails, which appear on a YouTube page. It's done with feed and newsfeed, where Facebook, in the hopes of keeping you online more, proffers to you materials which they think you'll be interested in.

Senator HAWLEY. So let me just ask you this. Does anything in the text of Section 230 as it was originally written, suggest, in your view, that platforms ought to get this really form of super immunity for promoting, taking other people's content, hosting it, promoting it, and in promoting it, making money off of it? I mean, does the statute immunize them from that? Does anything in the text support the super immunity in that way?

Professor SCHNAPPER. I spent a very long hour and a quarter trying to answer that question a few weeks ago. We think the text does draw that distinction. And that brings back so many happy memories that you ask that.

[Laughter.]

Professor SCHNAPPER. So yes, that's our view, but we're not here to retry the case. But that is our view of the meaning of the statute, but it doesn't—it would be entirely appropriate for the Committee to clarify that.

Senator HAWLEY. Let me just get to that point and finish my first round of questions with that. If Congress acts on this issue, what would be your recommendations for the best way to address this problem, from a policy legislative perspective? The problem you've identified in this case is about affirmative recommendations. How should we change the statute, reform the statute to address this problem?

Professor SCHNAPPER. I prefer not to try to frame legislative proposal as I sit here. It's complicated. And I'd be happy to work with your staff and my colleagues here, all of them, on that for you. But I think it would be inappropriate for me to start tossing out language as I sit here.

Chair BLUMENTHAL. Thanks, Professor Schnapper. Thanks, Senator Hawley. Senator Padilla.

Senator PADILLA. Thank you, Mr. Chair. I want to start out by asking consent to enter a letter into the record for more than three dozen public interest organizations, academics, legal advocates, and members of industry. A letter that notes, "In policy conversations, Section 230 is often portrayed by critics as a protection for a handful of large companies. In practice, it's a protection for the entire internet ecosystem."

Chair BLUMENTHAL. Without objection, your letter is made a part of the record.

[The information appears as a submission for the record.]

Senator PADILLA. Thank you. As we heard from the Supreme Court, this is a very thorny and nuanced issue, and we need to make sure that we treat it as such. Because of Section 230, we have an internet that is a democratizing force for speech, creativity, and entrepreneurship.

Marginalized and underserved communities have been able to break free of traditional media gatekeepers and communities have leveraged platforms to organize for civil rights and for human rights. But it's also important to recognize that there is a horrifying conduct and suffering that we can and must address.

My first question is for Professor Franks. In your testimony, you call for internet companies to more aggressively police their sites for harassment, hate speech, and other abhorrent conduct. And you recommend changes to Section 230 to compel that conduct. I share your concerns about the prevalence of this activity online.

Now, that said, I also know that many marginalized communities rely on platforms to organize. Many of the same communities fall prey to the automated and inaccurate tools employed by companies to enforce their content moderation policies at scale. Is it possible to amend Section 230 in a way that does not encourage providers to over-remove lawful speech, especially by users from marginalized groups?

Professor FRANKS. Thank you for this question. I'd first like to state that the current status quo where companies essentially have no liability for their decisions means that they can make any decisions that they would like, including ones that would harm dis-

proportionately marginalized groups. And so, while it is encouraging to see that some platforms have not done so, some platforms have behaved responsibly, some have even made it a commitment to in fact amplify marginalized voices.

These are all decisions that they are making essentially according to their own profit lines or according to their own motivations. And they can't really be relied upon as a guideline for how to run businesses that are so influential throughout our entire society.

So when I suggest that Section 230 should be changed, I do want to, again, emphasize the distinction between immunity versus the presence of liability, which is to say Section 230 presumably provides immunity from certain types of actions. That is not the same thing as saying you are responsible for those actions, if you are found not to have immunity.

So my suggestions are really directed towards asking the industry the same question that Justice Kagan has asked, which is, Why shouldn't this industry be just as subject to the constraints of potential litigation as any other industry? So, not that they should be treated worse, but that they should be treated the same as many other industries.

And that what that would hopefully do would be to incentivize these platforms to at least take some care in the way that they design their products and the way that they apply their policies, not to give them a sort of directive to say, this is how you have to do it, because you don't need a directive like that.

Essentially, what you need is to allow companies to act in a certain way. And if they do so in a way that contributes to harm and there is a plausible theory of liability, they should have to be accounted for that. But nothing preemptively that should allow them to say, "We are excused from this conduct, or that we are guilty of this conduct," but to simply change the incentive so that they have to sometimes worry about the possibility of being held accountable for their contribution to harm.

Senator PADILLA. Thank you. Next question is for Mr. Sullivan. Yesterday we had a Subcommittee hearing on competition policy that focused on digital markets. I want to make sure our legislative efforts to promote an open, innovative, equitable, and competitive internet harmonize with the platform accountability efforts here.

Notably, in response to questioning during oral arguments in *Google v. Gonzalez*, Google's attorney acknowledged that while Google might financially survive liability for some proposed conduct presented as a hypothetical, smaller players most definitely could not. Can you speak to the role Section 230 plays in fostering a competitive digital ecosystem?

Mr. SULLIVAN. Yes. Thank you for the question, because this is the core of why the Internet Society is so interested in this. This is precisely what the issue is. If there are changes to 230, it is almost certain that the very largest players will survive it because they've amassed so much wealth. But a small player is going to have a very difficult time getting into that market, and that's one of the big worries that I have.

You know, the internet is designed with no permanent favorites, and if we change the rules to make that favoritism permanent, it's going to be harmful for all of us.

Senator PADILLA. All right. Complex indeed. Thank you, Mr. Chair.

Chair BLUMENTHAL. Thanks, Senator Padilla. I'm going to call now on Senator Blackburn, who has been like Senator Hawley, a real leader in this area. She and I have co-sponsored the Kids Online Safety Act, which would provide real relief to parents and children, tools and safeguards they can use to take back control over their lives, and more transparency for the algorithms.

And then we will turn to Senator Klobuchar, who has been such a steadfast champion on reforming laws involving Big Tech, her SAFE TECH bill, as well as the competition bills that you mentioned, Mr. Sullivan, that I've been very privileged to help her lead on. Senator Blackburn.

Senator BLACKBURN. Thank you, Mr. Chairman. And this is one of those areas where we have bipartisan agreement. And as the Chairman said, I've worked on this issue of safety online for our children for quite a while, and for privacy for consumers when they're online, data security, as they've added more of their transactional life online.

And, Ms. Bennett, I think I want to come to you on this. When I was in the House and Chairman of Comms and Tech there, I passed FOSTA/SESTA, and that has been implemented. And we had so much bipartisan support around that and finally got the language right and finally got it passed and signed into law.

And some of the people that worked with us during that time have come to me recently and have said, "Hey, the courts are trying to block some of the victims' cases based on 230 language." And, Professor, I see you nodding your head also. I would like to hear from you what you see as what they have ascertained to be the problem, how we fix it if you think there is a fix, or is this just an excuse that you think they're using not to move these cases forward?

Ms. BENNETT. Sure. So I actually don't litigate FOSTA/SESTA cases. So if—was it Professor Franks who was nodding their head? I unfortunately don't know the answer to that for you, but I'd be happy to get it for you and could submit it afterwards.

Senator BLACKBURN. I would appreciate that.

Ms. BENNETT. I'd be very happy to get that.

Senator BLACKBURN. Go ahead, Professor.

Professor FARID. Yes. I'm not the lawyer in the room. I'm the computer scientist, but I will say I've seen the same arguments being made. I want to come back to something earlier too because I think this speaks to your question, Senator, about small platforms. Small platforms have small problems. They don't have big problems.

In fact, we have seen in Europe when we deploy more aggressive legislation, small companies comply quite easily. So I don't actually buy this argument that somehow regulation is going to squash the competition because they don't have big problems.

Coming back to your question, Senator Blackburn, we also saw—and I think this is important as we're talking about 230 reform—the same cries of, if you do this, you will destroy the internet. And it wasn't true. And so we can have modest regulation. We can put guardrails on the system and don't destroy the internet. I am see-

ing, by the way, and I don't know the legal cases, but I am seeing some pushback on enforcing SESTA/FOSTA and I think that's something Congress has to take up.

Senator BLACKBURN. Well, I think you're right about that. That's probably another thing that we'll need to revisit and update that as we look at children's online privacy in COPPA 2.0. Senator Markey, when we were in the house, led on that effort. And then, Senator Blumenthal and I have had the Kids Online Safety Act. Recently, Senator Ossoff and I introduced the REPORT Act, which would bolster NCMEC. And we think that's important to do. It would allow keeping CSAM info for a longer period of time so that these cases can actually be prosecuted.

And it's interesting that one of the things we've heard from some of the platforms is that changes to Section 230 would discourage the platforms from moderating for things like CSAM, and I would be interested from the professor, really from each of you, on the panel, if you believe that reforming 230 would be a disadvantage, that it would make it more difficult to stop CSAM and some of this information because it's amazing to me that changing—they think changing the law, being more explicit in language, removing some of the ambiguous language in 230 would be an incentive for the platforms to allow more rather than a disincentive. Ms. Franks, I'll start with you.

Professor FRANKS. Thank you. I think the clarity that we need here about Section 230 and about this criticism is to say, which part of Section 230, because if the objection is that changes to (c)(1), which is really the part of the statute that is being used so expansively, if the argument is that some of those changes would make it harder and would disincentivize companies from taking these kinds of steps, I'd say that's absolutely false.

(C)(2) quite clearly and expressly says this is exactly how you get immunity, is by restricting access to objectionable content. So what that means, of course, is that if it's a Section 230(c)(1) revision, you still have (c)(2)to encourage and to incentivize platforms to do the right thing.

That being said, potential attacks on (c)(2) could in fact have an effect on whether or not companies are properly incentivized to take down objectionable material. But there is, of course, also the First Amendment that would come into play here, too. Because as private companies, these companies have the right to take down, to ignore, to simply not associate with certain types of speech if they so choose.

Senator BLACKBURN. Okay. Professor, anything to add?

Professor FARID. I'll point out a couple of things here. I was part of the team back in 2008 that developed technology called PhotoDNA that is now used to find and remove child sexual abuse material, CSAM. That was in 2008.

That was after 5 years of asking, begging, pleading with the tech companies to do something about the most horrific content, and they didn't. It defies credibility that changes to 230 is going to make them less likely to do this. They came kicking and screaming to do the absolute bare minimum, and they've been dragging their feet for the last 10 years as well. So I agree with Professor Franks.

I don't think that this is what the problem is. I think they just don't want to do it because it's not profitable.

Senator BLACKBURN. Thank you. Ms. Bennett, anything to add?

Ms. BENNETT. I will do what everybody should always do, which is agree with Professor Farid and Professor Franks, which is, you know, to the extent we're talking about (c)(1), it shouldn't have any impact. If you're keeping the good-faith defense for removing content, then that's still there. And nothing, no changes to (c)(1) should impact that.

Senator BLACKBURN. Thank you. Mr. Sullivan.

Mr. SULLIVAN. While I agree with everything that has just been said, the truth of the matter is that this illustrates why this is such a complicated problem, because when you open the legislation, the chances that only one little piece of it is going to get changed, not so high. And so, the problem that we see is, you know, Section 230 is what gives the platforms the ability to do that kind of moderation. It's what protects them. And therefore, you know, we're concerned about the potential of, you know, for that to change as well.

Senator BLACKBURN. Okay. Professor?

Professor SCHNAPPER. I can't quite agree with everybody. It's gotten a little more complicated, but I think you can reform Section (c)(1) without creating disincentives to remove dangerous material. I think that's sort of a make-weight argument. I think you have to be careful about changes to (c)(2), although I understand that there are issues there.

But I just may bring home a point, I guess it was Professor Farid made. Spending money to remove dangerous material from a website is not a profit center. And I think Elon Musk has explained that to the country in exquisite detail. If there are no financial incentives to avoid harm, you don't make money by doing it, and you've got to change those incentives.

Senator BLACKBURN. I'm way over and I thank you for your indulgence.

Chair BLUMENTHAL. Thanks a lot, Senator Blackburn. Senator Klobuchar.

Senator KLOBUCHAR. Oh, thank you very much. And thank you to both you, Chair Blumenthal, and Senator Hawley for holding this hearing, Senator Blackburn for her good work in this area. So I was thinking Section 230 was enacted back in 1996. Probably there's just one or two remaining Members that were involved in leading that bill when we had dial-up modems accessing CompuServe. That's what we're dealing with here.

To say that the internet of 2023 is different from what legislators contemplated in 1996 is a drastic understatement. And yet, as I said at our Antitrust Subcommittee hearing yesterday, the largest dominant digital platforms have stopped everything that we have tried to do to update our laws to respond to the issues we are seeing from privacy to competition.

And like Senator Blumenthal, I—with the exception of the human trafficking that I'd been involved in early on—I was not crying for major changes to Section 230 either at the beginning. And part of what's brought me to this moment is the sheer opposition to every single thing we try to do.

Even when we tried, Lindsey Graham and I, before that Senator McCain did the Honest Ads Act to put disclaimers and disclosures, we got initial objection and then eventually some support, but it still hasn't passed the competition bills. The work even on algorithms.

The simple idea is that we should do some reforms to the app stores. This idea that we shouldn't be self-preferencing their own products when they have a 90 percent or a 40 percent market share, depending on which platform it is. The hypocrisy of things that we were told would break the internet that we now see them agreeing to do in Europe. That is the final dagger as far as I'm concerned and why you see shifting positions on Section 230.

Obviously, this is also a cry for some ability of the companies to come forward and actually propose some real reforms we can put into law, because so far it's just buy it all off with money, commercials, ads attacking those of us who have been trying to make a difference.

So my question, I guess, to you, Professor Farid, first is, they've said, "Trust us, we've got this," for so long. And the way the internet companies amplify content profit as Senator Hawley was explaining off of it, allowing criminal activity to persist on their platforms, we clearly need our reforms.

And I always think of it like if you yell "Fire" in a crowded theater, you know, the theater or multiplex, as long as they have nice exits, they aren't going to be liable. But if they broadcasted it in all their theaters, that would be called algorithms, that would be a different story.

You noted in your testimony that some legal arguments have conflated search algorithms with recommendation algorithms. Can you explain how these algorithms differ and their role in amplifying content on platforms?

Professor FARID. Good. Thank you, Senator. So if you go to Google or Bing and you search for whatever topic you want, your interests and the company's interests are very well-aligned. The company wants to deliver to you relevant content for your search, and you want relevant content, and we are aligned and they do a fairly good job of that. That is a search algorithm. It is trying to find information when you proactively go and search for something.

When you go to YouTube, however, to watch a video of a link that I sent you, you didn't ask for them to queue up another video. You didn't ask for the thumbnails down the right hand side. You didn't ask for any of that. And, in fact, you can't really turn any of that off. That's a recommendation algorithm. And the difference between the search algorithm where the company's interests and your interests are aligned, that is not true of recommendation algorithms. Recommendation algorithms are designed for one thing: to make the platform sticky, to make you coming back for more because the more time you spend on the platform, the more ads are delivered, the more money we make.

And if we're talking about harms, we've talked about terrorism, we've talked about child sexual abuse, we've talked about illegal drugs and illegal weapons, we should also talk about things like body image issues. We should talk about suicidal ideation.

Go to TikTok, go to Instagram. Start watching a few videos on one topic, and you get inundated with those. Why? That's because the recommendation is vacuuming up all your personal data and trying to figure out what is it that is going to bring you here over and over again.

Last thing on this issue, because it goes to knowledge, is that the Facebooks of the world, the YouTubes of the world know that the most conspiratorial, the most salacious, the most outrageous, the most hateful content drives user engagement. Their own internal studies have shown that as you drive content from cats, to lawful, to awful but lawful, and then across the violative line to illegal, engagement goes up.

And so, the algorithms have learned to recommend exactly the problematic content, because that is what it drives user engagement. We should have a conversation about what is wrong with us. Why do we keep clicking on this stuff? But the companies know that they are driving the most harmful content because it maximizes profit.

Senator KLOBUCHAR. Okay. Thank you. Professor Franks, kind of along those lines, circuit courts have interpreted Section 230 differently, with some saying that social media and internet companies are not liable for content that could only have been created with the tools they designed.

However, unlike most other companies that make dangerous or defective products, internet and social media companies are often shielded by Section 230 from cases that involve design defects. Should Congress consider reforming Section 230 to allow for design defect cases to move forward when a site is designed in a way that causes harm?

Professor FRANKS. Thank you. I think it would be, as I said with the other suggestion about revisions to Section 230, the concern I would have is about how exactly to codify that sort of standard. And I think that the impulse there is a good one. I think that the distinction between faulty design as opposed to simply recommendations or making access to other content, I think that is a solid distinction to make.

My concern is that the way—or, the best way and most efficient way to reform Section 230 is to try not to think about discreet categories of harmful content or conduct, but rather to talk about the underlying fundamental problem with Section 230, which is this idea that you should provide immunity in exchange for basically doing nothing or for even for accelerating or promoting harmful content.

Senator KLOBUCHAR. Yes, I agree. I was just trying to, you know, throw it out there. The last thing, how would reforms to Section 230, Professor Franks, create a safer internet for kids and where Congress should focus its efforts. We have a lot of things and talk a little bit about why that could be a priority.

Professor FRANKS. Well, one of the reasons that's a high priority is exactly for the reasons that Professor Farid has been speaking to, that those types of behavioral changes that we see that are essentially an intended consequence or an intended strategy on the part of companies to keep people on their platforms longer, to keep

them engaging with those platforms, these are dangerous for adults, but they're particularly pernicious for children.

This is a kind of approach that is essentially trying to encourage a form of addiction to these services. And it is part, I think, of what explains some of the very heightened rhetoric on the site, on the part of the tech industry and those who are convinced that the status quo is the best way forward. People identify so closely with their social media platforms at this point that any changes that are suggested to Section 230 feel like personal attacks.

And I think that that is a testament to how much Google and Facebook and TikTok, and every other company we can think of, is really striving and succeeding to make us feel that we cannot live without these products. That they're not products that we are using, but they're using us. And so, I think it is a particular importance and concern when this kind of effect is having on younger and younger children who have had really no time to develop their own personalities and their own principles.

Senator KLOBUCHAR. Okay. Thank you.

Chair BLUMENTHAL. Thanks, Senator Klobuchar. Senator Hirono.

Senator HIRONO. Thank you, Mr. Chairman. It's very clear that we want to make changes to Section 230, but there are always unintended consequences whenever we attempt to do that. There has been a lot of discussion of unintended consequences arising out of the SESTA/FOSTA.

Six workers have raised legitimate concerns about the consequences of that legislation and its effect on their safety. But that does not mean that we should shy away from reforming Section 230 to protect other marginalized groups. Just that we need to be very intentional about doing so and paying attention to the potential unattended consequences. This is for Professor Franks. Can you explain how the experience of SESTA/FOSTA should inform the types of reforms we should pursue?

Professor FRANKS. Thank you. I do think that SESTA/FOSTA is a good and instructive example of what can go wrong when Section 230 is amended. It, of course, had the very best of intentions. There were concerns, however, throughout the process that were coming from some of the individuals and groups who were saying, this kind of change is going to affect us most, and please listen to our concerns about how it should be done.

So I think that one lesson there is definitely to identify and to bring into the conversation the individuals who are most likely to be impacted by any form of reform. That's lesson one.

I think the other lesson is that this shows the dangers of attempting to highlight a certain category of bad behavior and try to carve that out into the statute as opposed to, as I said before, identifying the fundamentally flawed nature of Section 230 as it stands right now as it's interpreted by the courts and try to fix this on a more generalized level. Because I think the more particularized we tend to get with this, the more likely it is that we are going to make mistakes and have unintended consequences.

Senator HIRONO. Well, when you talk about not focusing on certain types of bad behaviors, but to look at the sort of the general problem with Section 230, so how would you make the kind of

changes that you're talking about to protect vulnerable communities?

Professor FRANKS. The two forms of amendment that I particularly suggest are changing the word "information" in (c)(1) to refer to "speech" instead. And the other is to limit (c)(1)'s protections to those who are not engaged in the knowledgeable promotion or contribution to unlawful content. I've suggested that the language there should be a deliberate indifferent standard because that is a standard that is used in other forms of third-party liability cases and areas.

And so, what I think would be useful about that approach, is that this is not an approach that's going to try to take one type of harm and say that that is more harmful than something else. But, rather, to say this is really how this form of liability tends to work in other industries and in other places.

And to be clear, not just industries that have very little to do with what the tech industry supposedly does, namely sometimes speech, but actually the industries that are very much about speech, including newspapers and television broadcasters and universities, all of whom have to be responsible at a certain level if they are deliberately indifferent to unlawful conduct.

Senator HIRONO. I think you were asked this question related to the SAFE TECH Act, which does talk about protecting speech rather than information. So are the other panelists aware of the provisions of the Safe Tech Act? And if so, any of you, would you agree that to protect speech is okay, but, you know, protecting information is not where we want to go? That may be one of the approaches that we should take to reforming Section 230. Would any one of the other panelists like to weigh in?

Professor SCHNAPPER. This may be too complicated to solve quite that way. Turning to Senator Klobuchar's point, it's not difficult to imagine it with lawyers putting back into the word speech, everything that the Committee thought it was taking out.

Senator HIRONO. Darn those lawyers. Okay. Yes, I realize that if we're going to make that kind of change, I think we need to provide more guidance as to what we mean by what we want to protect.

Again, for Professor Franks, one of the concerns I've had, particularly after the Supreme Court struck down a 50-year precedent and the right to abortion is that reproductive health data collected by these tech platforms may be used to target individuals seeking these services.

So these apps and websites are collecting location data, search histories, and other reproductive health information. And last Congress, I introduced My Body, My Data Act to help individuals protect private sexual health data. However, what I'm understanding is that though that Act creates a private right of action to allow individuals to hold regulated entities accountable for those violations, these tech platforms can currently just hide behind Section 230, even when put on notice that this information is being used for nefarious purposes, unintended purposes.

Based on your extensive legal experience, is there a way to hold tech companies disseminating reproductive health information from behind the shield of protection accountable?

Professor FRANKS. I think it's possible. I think that it would require moving away from this dominant interpretation of Section 230 as it currently stands.

Because that view of Section 230, that revision of (c)(1) as providing some sort of unqualified immunity to these platforms, really makes it difficult for any individual who is harmed in this way to even get their foot in the courtroom door.

And so, I think what we would need at this point is either a very wise decision from the Supreme Court about how to properly interpret (c)(1) and, or we would need Congress to clarify that once again, (c)(1) can be modified to make sure that it is clear, that these companies can in fact be sued if there is a plausible theory of liability and a causal connection between what those platforms did and the ultimate harm that is resulting to a plaintiff.

Senator HIRONO. It's not that easy for the plaintiff to show that, but she should have that opportunity, I would say.

Professor FRANKS. Exactly.

Senator HIRONO. Thank you. Thank you, Mr. Chair.

Chair BLUMENTHAL. Thanks, Senator Hirono. We may have other Members of the Subcommittee or our Committee come, but why don't we begin the second round of questions now and we can interrupt to accommodate them when they come here.

Let me just say to Dr. Franks, I appreciate your comments about SESTA, as one of the principal authors and co-sponsors. We endeavored to listen and we will change the statute if it has unintended consequences, and we will listen in the course of ongoing Section 230 reform, whether it's the EARN IT Act that Senator Graham and I are co-sponsoring. A number of us have proposals.

As I mentioned, Senator Klobuchar with the Safe Tech Act and Senator Hirono is a co-sponsor, as I am. Senator Hawley has a number of very promising proposals, but I think we should be very clear about what is really going on here. And, Professor Schnapper, I think you made reference to the money involved.

The fact of the matter is that Big Tech is making big bucks by driving content to people knowing of the harms that result. We saw that in the documents that were before the Commerce Subcommittee on Consumer Protection, that help support the Kids Online Safety Act. More eyeballs for longer periods of time mean more money. And Big Tech may be neutral or indifferent on the topic of eating disorders, suicide or bullying or other harms. They may not want to take out an ad saying, engage in these activities, but they know that repeating it and amplifying it, and in fact, addicting kids to this kind of content has certain consequences. And as Justice Kagan said, "Why should Big Tech be given a pass?"

An airline, Boeing, that has a faulty device that causes the plane to nose-dive, a car company like GM that has a defective ignition switch that causes the car to stop and go off the road, they're held responsible. Why shouldn't Big Tech be held responsible? Whether the standard's deliberate indifference or some other standard? It may be difficult, it may be complicated, but it's hardly impossible to impose a standard.

So let me ask you, Mr. Sullivan, what's your solution here? I'm asking Big Tech to be part of the solution, not just the problem.

Mr. SULLIVAN. Well, let me be clear that I can't speak for Big Tech because I work for a nonprofit.

Chair BLUMENTHAL. Well, I'm asking then.

Mr. SULLIVAN. But we have, you know, our concern is really what users need. Our concern is really what people need. And what we are trying to point out is that 230 is the thing that allows the internet to exist. So I am not here to say that the behavior that we see, the behavior of various large tech corporations, the behavior of some platforms, you know, that are perhaps outside of the United States for that matter, that those are all unproblematic. There are definitely problems there.

What I'm suggesting is that a narrow application, the attacking of this narrow piece of legislation is going to harm the internet in various ways. And so, if you want to do something about large corporations, for instance, then you've got an issue having to do with industrial policy. It's not an issue to do actually with the internet. And it seems to me that, you know, these concerns are legitimate ones, but I think we're trying to go after the wrong tool.

Chair BLUMENTHAL. Well, the tool can't be just more competition. The tool can't be more privacy, as you've suggested in your opening comments. It has to be something dealing with this harm. And as I have said before, I'll say again, the carve-outs, the limits that have been imposed so far, whether it's *Henderson* or *Lemmon* or other caselaw, haven't broken the internet. I don't think you can argue that Section 230 as it exists right now is essential to continuing the internet. That's not your position. Is it?

Mr. SULLIVAN. I think that Section 230 is a critical part of keeping the internet that we have built. And the reason I think that is because it protects people in those interactions. It protects from that kind of third-party liability. I am not, you know, I'm not here to suggest that it is logically impossible to find a particular carve-out from 230 that will help solve some of these problems.

I haven't seen one yet, and so I'm very skeptical that we're going to get one. But I am not here to suggest that it's logically impossible. I'm just very concerned that we understand the potential to do a lot of harm to the internet. When people say destroy the internet, I think that this, you know, this sounds like an on-off switch, but that's not how the internet works.

And we can either drift in the direction of losing the advantages of the internet, losing the interactivity, losing the ability of users to have the experience that they need online and in favor of a centrally controlled system. And that is the thing that I'm mostly concerned about.

Chair BLUMENTHAL. So taking the Kids Online Safety Act, which simply requires these tech platforms to enable and inform parents and children, they can disconnect from the algorithms. And if they do something, you know, let's use some non-legal term, something really outrageous, and they violate a basic duty of care, which under our common law is centuries old, they can be held liable.

And as Senator Hawley said so well, they get a day in court. That's fundamental to our system. I don't understand why there would be harms inevitably as a result of that kind of change.

Mr. SULLIVAN. The concern that I have is that, you know, in the United States, it's easy to initiate a lawsuit and it's expensive and

complicated to defend against it. So very, very large players, incumbents that we have today, the people who are, you know, the richest corporations in the history of capital, they have the resources to do this.

But if you are like a community website, you know, or a church website and you allow discussions on there and somebody comes on and they start doing terrible things, you're going to end up with the exact same liability and that will gradually turn down the ability of the internet to connect people to one another. That's what I am concerned about.

You know, I mean, I'm not carrying any water for a giant tech corporation. I don't work for one, and I can't really, you know, influence their direction. But my point is that the way 230 works right now, it protects all of the interaction on the internet. And if we lose that, we will most certainly lose the internet. We'll still have something we call the internet for sure, but it will not be the thing that allows people to reach out and connect to one another. All of these terrible harms, all of these terrible things that happen online, there are corresponding examples of people getting help online.

Chair BLUMENTHAL. I appreciate your concern about the community websites, but they're not the ones driving suicidal ideation or bullying or eating disorders to kids. And I understand that Section 230 dates from a time when the internet was young and small. Nobody's forever young, and these companies are no longer small.

They're among the most resourced of any companies in the history of capitalism. And for them of all companies to have this free pass, as Justice Kagan called it, seems to me not only ironic, but unacceptable. And again, what's at stake here ultimately are the dollars and cents that these companies are able to make by elevating content.

And I sort of am reminded of Big Tobacco, which said, "Oh, we're not interested in kids. We don't advertise to them. We don't promote our products to children." And of course, their files, like Facebook's files, showed just the opposite. They knew what they were doing in order to raise their profits, and they put profits over those children.

So I think, again, I'm hoping, not talking to you personally, but to the internet world out there and the tech companies that have the resources and responsibility, they will be a constructive part of this conversation. Thank you.

Senator HAWLEY. You know, isn't the best—let me just pose this question on the panel. Maybe I should start with you, Professor Franks, but isn't the best way to address the many abuses that we're seeing by the Big Tech companies, and we've talked about some of them today—with CSAM, Professor Farid, you mentioned CSAM, that's got to be one of the leading ones. I'm a father of three children, all of them very small. I worry about this every day—my oldest is 10—as they get old enough to want to be on the internet.

There are other abuses, the videos that promote suicide, the videos that promote violence, and we could go on and on. Isn't the best way to deal with that just to allow people to get into court and hold these companies accountable? Here's what I've learned in my short time in the Senate, is that we can write regulations and we can

give the various regulatory agencies the power, whether it's the FTC or others, the power to enforce them.

But my experience is, my observation is, is that the Big Tech companies tend to own the regulators at the end of the day. I mean no offense to any of the regulators who are watching this, but, you know, you know I'm right. At the end of the day, it's a revolving door. They go to work for the Big Tech companies. They come out of employment and go into the Government. And it's just amazing how the regulators always seem to end up on the side of tech.

And for that matter, even when they do fine tech, even if it's a big fine, Meta got fined, I think, a billion dollars a couple years ago. They didn't care. Didn't change anything. That's nothing to them. The revenues are massive. Their profits are massive. But what strikes fear into their hearts is if you say, "Oh, but we'll allow plaintiffs to go to court."

Take the Big Tobacco example. What finally changed the behavior of Big Tobacco? Lawsuits. Normal people got into court, class action suits. So isn't that really what we're talk—just to simplify this, isn't that what we're really talking about today?

I mean, the thing that we ought to be doing is figuring out a way, and you proposed a way, Professor Franks. I was just reviewing your written testimony here a second ago with the changes you would make to the statute. But the gist of that is to create a system and a standard that is equitable in terms of being, it's the same across the board for everybody. You don't single out one particular piece of conduct. You would just change the standard. But the point of it is, people would be able to be using this standard to get into court, to have their day in court, and to hold these companies accountable. Is that fair to say? Is that too simplified?

Professor FRANKS. I think that is fair to say, that as you're pointing out, litigation is one of the most powerful ways to change an industry. And it's not just because of the ultimate outcome of those cases, but also because of the discovery in those cases. What we get to see instead of having to wait for whistleblowers or wait for journalists, is actually the documents themselves, internal documents about what you knew, when you knew it, and what you were doing.

And so, I think that exactly for this reason, we have to be interpreting Section 230 as not providing some kind of supercharged immunity that no other industry gets, but actually, yes, allow people who have been harmed to get into court, make their claim. They may not prevail, they might. But at any event, we will see some public service also in terms of the discovery process that shows us what these companies are doing and to the tune of how much money.

Because a lot of what is being said about the distinctions between the big corporations and the little ones, how did the big corporations get so big? Because they didn't get sued. And so, if we care about that kind of monopolization, if we care about that kind of disproportionate influence, what will benefit the entire market is actually letting those companies be sued if they have caused harm.

Senator HAWLEY. Yes, I couldn't agree more. And with all due respect to you, Mr. Sullivan, I know you have an obligation to represent the people for whom you work, but I would just say it's pret-

ty hard to argue that the social media landscape, the social media industry right now, for example, is a good example of a competitive industry.

It's not particularly competitive at all. It's controlled overwhelmingly by one or two players. It is the very quintessence of monopoly. I mean, you have to go back over a century in this country's history to find similar monopolization. And to Professor Franks' point, I think you can make a very strong argument that Section 230 and the incredible immunity that it has provided for a handful of players has contributed to this monopolization. It is in effect a massive Government subsidy to the tune of billions of dollars a year.

So I'll just say that, listen, as a conservative Republican, I mean, I want to be clear about this. I am a conservative Republican. I believe in markets. I'm skeptical of massive regulatory agencies, but one of the reasons I'm skeptical is I just see them get captured time, after time, after time. But I believe in the right of people to be heard and to be vindicated and to have their days in court.

And I think the best way you protect the little guy and give him the power or her the power to take on the big guy, is allow them into court, let them get discovery, let them hire a tort lawyer, let them bring their suits. And you're right, Professor Franks, maybe they win, maybe they don't, but that's justice, right? It'll be a fair, even-handed standard.

The last thing I would say is that, I think that's actually much closer to what Section 230, when Congress wrote it, was meant to be. If you look at the language of 230, you know, it's interpreted by courts to provide this super immunity, as you were saying, Professor Franks. I think it's very arguable, and this is the argument I made in the Google case of my amicus brief, was that listen, what it really was meant to do is preserve distributor liability.

There's a baseline at the common law of distributor liability that says if a distributor who doesn't originate the speech, but merely hosted and distributes it, they can't be liable for somebody else's speech and shouldn't be. I think we all agree on that. Only if they promote speech that they know is unlawful or should have known as unlawful, regardless of the nature of the speech. Which gets to your point, Professor Franks, you know, whatever category you want.

If it's unlawful, they know it, they should have known it, then under traditional distributor liability, then and only then they can be liable. But what has happened is, the courts have obviously swept that away completely now too, and 230 bars even that form of liability. Surely we can agree that there should be—whether it's the standard you propose Professor Franks, which I think is pretty close actually to traditional distributor liability.

We could find a way to allow people to have their basic claims vindicated to hold accountable these companies when they are actively promoting harmful content that they know or should know is harmful.

And I would just submit that's the best way forward here, and I look forward with working with the Chairman here as we continue to gather information and try to put forward proposals that will do that in a meaningful way. Thank you, Mr. Chairman.

Chair BLUMENTHAL. Thanks a lot, Senator Hawley. I have another question or two relating to AI. We haven't really talked about it specifically in much detail, but obviously Americans are learning for the first time with growing fascination and some dread about ChatGPT and Microsoft Bing passing law school exams and making threats to users, both fascinating and pretty unsettling in some instances.

And some of what's unsettling involves potential discrimination. There's a study from Northeastern University, Harvard, the nonprofit Upturn—studies by them finding that some of Facebook's advertising discriminates on the basis of gender, race, and other categories. Maybe I could ask the panel whether those threats, beginning with you, Professor Franks, are distinct or whether they're part of this algorithm threat that we see generally involving some of these tech platforms.

Professor FRANKS. With the caveat that I'm not an AI expert by any means, I think I would reiterate my position that my concern about approaches that try to parse whether something is an algorithm or whether something is artificial intelligence or whether something is troubling from a different perspective, I would rather the conversation be about, again, the fundamental flaws and the incentive structure that Section 230 promotes, rather than trying to figure out whether one particular category or another is presenting a different kind of harm.

I think the better approach is to look at that fundamental incentive structure and ensure that these companies are not getting unqualified immunity.

Chair BLUMENTHAL. Professor Farid.

Professor FARID. There's a lot that can be said on this topic, Senator Blumenthal. I'll say just two things here. One is we are surely but quickly turning over important decision-making to algorithms, whether they are traditional AI or machine learning or whatever it is.

So, for example, the courts are using algorithms to determine if somebody is likely to commit a crime in the future and perhaps deny them bail. The financial institutions have, for decades, used algorithms to determine whether you get a mortgage or a small business loan.

Medical institutions, insurance companies, employers are now, more likely than not, the young people sitting behind you when they go to apply for a job, will sit in front of a camera and have an AI system determine if they should even get an interview or not. And I don't think it's going to surprise you to learn that these algorithms have some problems. They are biased. They are biased against women. They are biased against people of color.

And we are unleashing them in these black box systems that we don't understand them, we don't understand the accuracies, we don't understand the false alarm rates, and that should alarm all of us. And I haven't gotten to the ChatGPTs of the world yet, or the deepfake yet.

So the second thing I want to say about this, is there's going to be something interesting here around 230 and generative AI, as we call it. So generative AI is ChatGPT, OpenAI's DALL•E, the image synthesis, and deepfakes.

Let's say we concede the point that platforms get immunity for third-party content, but if the platforms start generating content with AI systems, as Microsoft is doing, as Google is doing, and as other platforms are doing, there's no immunity. This is not third-party content.

If your ChatGPT convinces somebody to go off and harm themselves or somebody else, you don't have immunity. This is your content. And so, we have to—I think the platforms have to think very carefully here. More broadly, we need to think very carefully how we are deploying AI very fast and very aggressively. The Europeans have been moving quite aggressively on this. There is legislation being worked on in Brussels to try to think about how we can regulate AI while encouraging innovation, but also mitigating some of the harms that we know are coming and have already come to our citizens.

Chair BLUMENTHAL. Thank you very much. Important points. Ms. Bennett.

Ms. BENNETT. So your question, is there anything fundamentally different? I think with respect to 230 with these different kinds of technologies and with the same caveat as Professor Franks gave, which is I'm not an AI expert, you know, I think the answer is no. And the fundamental distinction here is, are we trying to impose liability on these companies for something someone else said? So, because Facebook allowed somebody to post something?

Or, is the harm really caused by something the company itself is doing? You know, there have been claims against Facebook, for example, that it differentially provides ads on insurance and housing and things like that, by race or by gender or by age.

And the problem there isn't the housing ad. The housing ad is fine. The problem is the distribution to by race or by age or by gender. The harm is being caused by what the platform is doing, not by the content.

And I think that's true. You know, you see that ChatGPT. You know, similar principles. The harm isn't what people are putting into ChatGPT. It's what ChatGPT might spit out. And there again, it's the conduct of the platform itself. And so, I think the principles apply, you know, no matter what the technology is, this distinction between content that somebody else put on the internet and what the platform itself has done.

Chair BLUMENTHAL. Mr. Sullivan

Mr. SULLIVAN. I think that's broadly right. More importantly, I don't really think that AI is fundamentally a part of the internet. It's just a thing that happens to use it a lot of the time. But the reality under those circumstances is it's another piece of content. Somebody else has made it. And so, for 230 purposes, I don't think it's—I don't think it's part of the conversation.

Chair BLUMENTHAL. Professor.

Professor SCHNAPPER. I just add that it's my understanding that to some degree, AI is in place now. That is when these algorithms were constantly being tweaked to be more effective, and some of it's done by software engineers, but some of it is machine learning. As the software discovers what works and what doesn't, it changes what it does. That's been going on for some time.

Chair BLUMENTHAL. Thank you. Well, I think that that last question shows some of the complexity here. I'm not sure we all agree that AI is totally distinguishable. I guess it depends on how you define AI and algorithms. But I do think that we can make a start on reforming Section 230 without waiting for a comprehensive or precise definition of AI.

And I want to thank this panel. It's been very, very informative and enlightening and very, very helpful. We've had a good turnout and many of you have come from across the country. Really appreciate it. And the record is going to be held open for 1 week in case there are any written statements or questions from Members of the Subcommittee.

I really do thank you and we are going to be back in touch with you, I'm sure, as we proceed, but have no doubt we are moving forward. I think the bipartisan showing here and the bipartisan unanimity that we need change is probably the biggest takeaway. And I think we are finally at a point where we could well see action.

Can't predict it with certainty. Some of it will depend on the cooperation from the tech platforms and social media companies that have a stake in these issues. But I'm hoping they will be constructive and helpful. And you have certainly been all of that today. Thank you so much. This hearing is now adjourned.

[Whereupon, at 3:51 p.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Witness List
Hearing before the
Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, & the Law

"Platform Accountability: *Gonzalez* and Reform"

Wednesday, March 8, 2023
Dirksen Senate Office Building, Room 226
2:00 p.m.

Mary Anne Franks
Professor of Law and Michael R. Klein Scholar Chair
University of Miami School of Law
Miami, FL

Hany Farid
Professor, School of Information and Electrical Engineering and Computer Science
University of California, Berkley
Berkeley, CA

Jennifer Bennett
Principal
Gupta Wessler PLLC
San Francisco, CA

Andrew Sullivan
President and CEO
Internet Society
Reston, VA

Eric Schnapper
Professor of Law
University of Washington School of Law
Seattle, WA

Statement of Jennifer Bennett
Principal, Gupta Wessler PLLC, San Francisco, CA

Before the United States Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law

"Platform Accountability: *Gonzalez* and Reform"

March 8, 2023

Chair Blumenthal, Ranking Member Hawley, and distinguished members of the Subcommittee, thank you for the opportunity to appear before you today. I am a principal at Gupta Wessler PLLC, a law firm focused on Supreme Court and appellate advocacy in the public interest. I have appeared before trial and appellate courts across the country, both state and federal, as well as the U.S. Supreme Court on behalf of workers, consumers, and civil-rights plaintiffs.

Although the title of this hearing references *Gonzalez v. Google*, I've been invited here today to discuss another Section 230 case: *Henderson v. Public Data*, an appeal that I recently argued before the Fourth Circuit. And the reason that case is interesting is because the one thing all of the litigants in *Gonzalez* seemed to agree on is that the decision in that case is correct.[1] So in thinking about what Section 230 means and how it might clarified, *Henderson* is a useful starting point.

I will explain the court's decision in more detail. But the bottom line is that *Henderson* focuses on a key distinction—and this is the distinction I think everyone is agreeing with when they say *Henderson* is correct. That key distinction is between liability based solely on the content that a platform's users have posted—the core of what Section 230 is designed to protect against—and liability based on the platform's *own* conduct, which Section 230 does not shield.

Background. Before diving into the decision, a bit of background on the case: The defendant in *Henderson* is Public Data, an online background check company. As alleged in the complaint, the company buys personal data about people across the country—including criminal records, court records, and DMV records—much of which is governed by laws restricting its distribution. And it uses this data to compile

---

[1] *See* Oral Arg. Tr. 3 (petitioners' counsel stating that "*Henderson* correctly interprets the statute"); *id.* at 144 (respondent's counsel stating that *Henderson*'s "test is correct"); United States Br. 16 (discussing *Henderson* with approval). The oral argument transcript is available at https://www.supremecourt.gov/oral_arguments/argument_transcripts/2022/21-1333_p8k0.pdf. The Government's amicus brief is available at https://www.supremecourt.gov/DocketPDF/21/21-1333/249441/20221207203557042_21-1333tsacUnitedStates.pdf.

its own "original, proprietary" background check reports, which it then sells online to employers, landlords, and lenders.[2]

In creating these reports, Public Data does not merely regurgitate the records it buys verbatim. Instead, it aggregates the data it acquires, "parse[s]" it, "strip[s] out" much of the information contained in actual court records, and replaces that information with its own "glib" not-always-accurate statements purporting to summarize a person's criminal history. Public Data's customers then use these reports to make crucial decisions on everything from hiring to renting to creditworthiness.

Background screening, like that provided by Public Data, is a multi-billion-dollar industry. Over ninety percent of employers and landlords use background checks to evaluate prospective tenants and employees. So a background-check error—a false criminal conviction, for example—can make it impossible to find work or housing. For that reason, the Fair Credit Reporting Act requires that companies that provide background checks (and other consumer reports) follow procedures designed to ensure that people are aware of the information being provided to employers and landlords about them; that employers that buy this information have consent to do so; and that the information consumer reporting agencies sell is as accurate as possible.[3]

But Public Data has chosen not to comply with the Fair Credit Reporting Act. The *Henderson* case arose out of this choice. The lawsuit was brought by Tyrone Henderson, George Harrison, and Robert McBride, Virginians who have lost housing or employment opportunities because of inaccurate information reported about them in their background checks. Background checks on Mr. Henderson, for example, often report that he has a felony history that is not, in fact, his, but rather that of another person with a similar name. Public Data's background check for Mr. McBride listed multiple criminal offenses, for which he was never actually prosecuted.

In an attempt to determine whether their background checks were accurate, Mr. Henderson, Mr. Harrison, and Mr. McBride each requested a copy of their files from Public Data. Although the Fair Credit Reporting Act requires consumer reporting agencies to provide consumers' files upon request, Public Data refused. The company also did not notify Mr. McBride when it provided its (inaccurate) background check to a potential employer—despite the Fair Credit Reporting Act's requirement that it do so. And Public Data does not require that employers certify

---

[2] Unless otherwise specified, all of the factual allegations and quotations in this section are drawn from the second amended complaint in *Henderson*, which is available at Docket No. 56, Case No. 20-294 (E.D. Va.).

[3] *See* 15 U.S.C. §§ 1681g, 1681k(a), 1681b(b)(1), 1681e(b).

that they have the permission of the person whose background check they're seeking to procure, nor does it require employers to certify that the information will not be used in violation of the law—even though the Fair Credit Reporting Act prohibits selling background checks to employers without these certifications.

Mr. Henderson, Mr. Harrison, and Mr. McBride, therefore, sued Public Data for its violations of the Fair Credit Reporting Act. In response, Public Data argued that because it operates online, Section 230 immunizes it from claims brought under the statute. Its argument was opposed by a broad, diverse coalition of *amici* including the State of Texas, as well as twenty other states, the Consumer Financial Protection Bureau and the Federal Trade Commission, consumer protection groups, workers' rights groups, and civil rights groups.

The Fourth Circuit rejected the contention that Section 230 immunizes Public Data from Fair Credit Reporting Act claims, simply because the company operates online. Section 230 provides 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."[4] By its terms, the Fourth Circuit explained, the statute only shields online companies from claims that (1) treat them as the publisher of (2) content "provided by another information content provider." The claims in *Henderson*, the court held, didn't satisfy these requirements. Section 230, therefore, did not shield Public Data from liability. And in explaining why, the court gave voice to what seems to be a growing consensus view about what Section 230 means.[5]

"Treated as the publisher." The *Henderson* court started by considering what it means for a claim to treat an internet company as a publisher. The court explained that "the term publisher as used in § 230(c)(1) derives its legal significance from the context of defamation law." That's because the purpose of Section 230 was to overrule *Stratton Oakmont*, a defamation case that had imposed liability on an internet platform for its users' postings, simply because the platform had made an effort to take down offensive posts. That effort, *Stratton Oakmont* held, rendered the platform a publisher liable for its users' speech. The point of Section 230 is to prevent this kind of liability. So when the statute bars claims that treat an internet company as a publisher, it's referring to claims that impose publisher liability as that term was understood in common law defamation claims—like the claims in *Stratton Oakmont*.

---

[4] 47 U.S.C. § 230(c)(1).

[5] The Fourth Circuit's opinion is available at *Henderson v. Source for Pub. Data, L.P.*, 53 F.4th 110 (4th Cir. 2022). Unless otherwise specified, all internal quotation marks, citations, and alterations are omitted from quotations of the case, as well as other quotations in this statement.

The Fourth Circuit in *Henderson* explained that at common law, publisher liability had two requirements. First, a publisher was someone who disseminated information to third parties. But information dissemination "was not enough." There was a second requirement for publisher liability: improper content. "[T]o hold someone liable as a publisher at common law was to hold them responsible for the . . . improper character" of the content they published.

Thus, the court held, "a claim only treats" an online platform as a publisher under Section 230, "if it (1) bases the defendant's liability on the disseminating of information to third parties and (2) imposes liability based on the information's improper content." Based on this plain-text, historical reading of Section 230, the court rejected the argument that Section 230 immunizes platforms from any claim that "hinges in any way on the act of publishing"—or, put in legal terms, any claim in which "publication [is] a but-for cause of the [plaintiff's] harm." That's not what publisher liability meant when Section 230 was enacted—and so it's not what Section 230 means when it prohibits treating a platform as a publisher.

Applying this understanding to the claims in *Henderson*, the court held that Section 230 "does not provide blanket protection" from all Fair Credit Reporting Act claims simply because the Act only applies to companies that publish credit information. The relevant question is—with respect to "each specific claim"—whether that claim (1) holds someone liable for disseminating information to third parties (2) based on that information's improper content.

The court's application of that test to the claims in *Henderson* is instructive. The plaintiffs' claim that Public Data failed to provide them a copy of their file, the court held, did not treat the company as a publisher because it failed prong 1 of the publisher liability test: dissemination to a third party. The claim was based on Public Data's failure to disseminate information to the subject of that information—not someone else. The plaintiffs' claim that Public Data unlawfully sold background checks without requiring purchasers to certify they had permission and a proper purpose, the court held, failed prong 2 of the publisher liability test: improper content. The claim didn't depend in any way on the propriety of the data Public Data published; it was based solely on Public Data's failure to obtain the proper certifications before doing so. On the other hand, the court suggested that any claims that sought to hold an online company liable because the background checks it sold were inaccurate, could potentially be understood as treating the company as a publisher within the meaning of Section 230.[6] That's because those claims would seek to impose liability for disseminating improper content to third parties.

[6] The court did not actually decide the issue.

Put simply, *Henderson* draws a clear line between imposing liability because a platform disseminates unlawful content and imposing liability for the platform's conduct. Only the former treats the platform as a publisher.

"Provided by another information content provider." But, as *Henderson* explains, Section 230 does not immunize online companies even from all claims that treat them as a publisher. It protects platforms only from those claims that would treat them as "the publisher" of "information provided by *another* information content provider."[7] In turn, the statute defines "information content provider" as someone "responsible, in whole or in part, for the creation or development of information provided through the Internet."[8] Courts agree, therefore, that Section 230 does not immunize companies for any content that they themselves are "responsible" for creating or developing, even "in part."

Here, too, *Henderson*'s analysis is informative. *Henderson* explains the widespread agreement among courts that, at the very least, a platform "develop[s]" content—and therefore falls outside of Section 230's protection—when its "own actions contribute[ ] in a material way" to what makes the content improper. Thus, the court held that Section 230 did not shield Public Data from claims that, in publishing data it collected from others, the company "omitted or summarized information in a way that made it misleading." Doing so, the court explained, goes beyond the kind of "formatting" or "procedural alterations" necessary to enable a platform to publish third-party content and makes the platform itself responsible—at least in part—for the content.

This line accords with the purpose of Section 230. The statute "prevents suits that cast [an online platform] in the same position as the party who originally posted the offensive messages." That is, it prevents lawsuits that merely seek to impose "vicarious liability" on a platform for its users' speech. But it does not shield online companies "when the offensiveness" of the content stems from the platform itself.

Growing consensus. *Henderson* does not stand alone. There is a growing consensus that Section 230 does not—and was never intended to—shield a platform from liability for its own conduct.[9] Take, for example, the Ninth Circuit's decision in *Lemmon v. Snap*. In that case, the parents of two teenagers who died in a car accident sued Snap, a social media company, alleging that the accident was caused by Snap's negligent design of its cellphone app, SnapChat. According to the parents, SnapChat incentivizes users to send videos and photos (called "snaps") to other

---

[7] 47 U.S.C. § 230(c)(1) (emphasis added).

[8] *Id.* § 230(f)(3).

[9] *See, e.g., Lemmon v. Snap, Inc.*, 995 F.3d 1085 (9th Cir. 2021); *Fed. Trade Comm'n v. LeadClick Media, LLC*, 838 F.3d 158 (2d Cir. 2016); *F.T.C. v. Accusearch Inc.*, 570 F.3d 1187 (10th Cir. 2009) *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008) (en banc); *Brooks v. Thomson Reuters Corp.*, 2021 WL 3621837 (N.D. Cal. Aug. 16, 2021).

users on the platform by rewarding them based on the snaps they send. SnapChat also offers users a "Speed Filter," which allows them to capture how fast they are going and overlay that information onto a video or photo. The parents alleged that SnapChat knew that its users believed the app would reward them for recording a snap at 100 miles per hour or faster and sharing it on the platform, and thus that it was leading young drivers to drive dangerously fast. In fact, there had been a series of news articles about the danger, other accidents, and even a previous lawsuit. In other words, the parents alleged that Snap designed an application that incentivized dangerous driving, knew that the app was causing accidents, and yet refused to do anything about it.[10]

In response, Snap argued that Section 230 protected it from liability. The Ninth Circuit rejected the argument for similar reasons that *Henderson* rejected Public Data's Section 230 argument. *First*, the court held that the parents' negligent-design claim didn't treat Snap as a publisher. It didn't seek to hold the company liable for improper content; it sought to hold the company liable for designing a dangerous product. "The duty to design a reasonably safe product is fully independent of Snap's role in monitoring or publishing third-party content." *Second*, the court held that the parents' claim didn't seek to hold Snap liable for third-party content. The basis of their claim was Snap's own design choices: its own architecture, its own "Speed Filter," its own rewards system.

Stepping back, the court explained, Snap "is an internet publishing business. Without publishing user content, it would not exist." But just because "publishing content" is a "cause of just about everything" Snap does, that doesn't mean that Section 230 shields Snap from all liability. Section 230 "was not meant to create a lawless no-man's-land on the Internet." It shields platforms from claims against them based on the speech their users publish; it does not immunize companies for their "own acts."

Conclusion. The litigants in *Gonzalez v. Google* disagree about virtually everything except that *Henderson* provides the correct framework for analyzing claims of immunity under Section 230. As this subcommittee, and Congress more generally, considers Section 230, *Henderson* provides a blueprint for what Section 230 was always meant to be: a shield from liability based on internet users' content, not platforms' own conduct.

* * *

Thank you again for the opportunity to testify today. I look forward to your questions.

---

[10] The Ninth Circuit's decision is available at *Lemmon v. Snap, Inc.*, 995 F.3d 1085 (9th Cir. 2021).

42

Senate Judiciary
Platform Accountability: Gonzalez and Reform

Hany Farid, Ph.D.

Biography

Hany Farid is a Professor at the University of California, Berkeley with a joint appointment in Electrical Engineering & Computer Sciences and the School of Information. His research focuses on digital forensics, online harms, image analysis, and human perception. He received his undergraduate degree in Computer Science and Applied Mathematics from the University of Rochester in 1989, his M.S. in Computer Science from SUNY Albany, and his Ph.D. in Computer Science from the University of Pennsylvania in 1997. Following a two-year post-doctoral fellowship in Brain and Cognitive Sciences at MIT, he joined the faculty at Dartmouth College in 1999 where he remained until 2019. He is the recipient of an Alfred P. Sloan Fellowship, a John Simon Guggenheim Fellowship, and is a Fellow of the National Academy of Inventors.

Testimony

Background

In the summer of 2017, three Wisconsin teenagers were killed in a high-speed car crash. At the time of the crash, the boys were recording their speed of 123 mph on Snapchat's *Speed Filter*. This was not the first such incident. A 2015 crash left a Georgia man with permanent brain damage. Also in 2015 the *Speed Filter* was linked to the death of three young women in Philadelphia. And in 2017, five people in Florida died in a high-speed collision, which again reportedly involved the *Speed Filter*.

Following the 2017 tragedy, parents of the passengers sued Snapchat claiming that their product, which awarded "trophies, streaks, and social recognition,"

was negligently designed to encourage dangerous high-speed driving. In 2021, the Ninth Circuit ruled in favor of the parents and reversed a lower court's ruling that had previously emphasized the *Speed Filter* as creating third-party content and was thus deserving of Section 230 protection.

Section 230 immunizes platforms in that they cannot be treated as a publisher or speaker of third-party content. In this case, however, the Ninth Circuit found that plaintiff's claims did not seek to hold Snapchat liable for third-party content, but rather for a faulty product design which predictably encouraged dangerous behavior. In response, Snapchat removed the *Speed Filter*.

This landmark case – *Lemmon v. Snap* – made a critical distinction between a product's negligent design decisions and the underlying user-generated content.

Gonzalez

Frustratingly, over the past several years, most of the discussions of Section 230 – and most recently, in the US Supreme Court oral arguments in *Gonzalez v. Google* – this fundamental distinction between content and design has been overlooked and muddled.

At the heart of *Gonzalez* is whether Section 230 immunizes YouTube when they not only host third-party content, but make targeted recommendations of content. Google's attorneys argued that fundamental to organizing the world's information is the need to algorithmically sort and prioritize content. In this argument, however, they conflated a search feature with a recommendation feature. In the former, the algorithmic ordering of content is critical to the functioning of a Google search. In the latter, however, YouTube's *Watch Next* and *Recommended for You* features – which lie at the core of *Gonzalez* – are fundamental design decisions that materially contribute to the product's safety.

The core functionality of YouTube as a video-sharing site is to allow users to upload videos and allow other users to view and possibly search for videos. The basic functionality of recommending videos after a video is watched (*Watch Next*) and enumerating a list of recommended videos alongside each hosted video (*Recommended for You*) is a design decision made to increase user engagement and, in turn, ad revenue. While optimizing for these features may seem innocuous, this design decision has a critical safety flaw.

YouTube has argued that their recommendation algorithms are neutral in that they operate in the same way as it pertains to cat videos and ISIS videos. This is not the point. Because YouTube cannot distinguish between cat and ISIS videos, they have negligently designed their recommendation feature and should remove it until it operates accurately and safely.

YouTube has also argued that with 500 hours of video uploaded every minute, they must make decisions on how to organize this massive amount of content. But again, searching for a video based on a creator or topic is distinct from YouTube's design of a recommendation feature where its sole purpose is to increase YouTube's profits by encouraging users to binge watch more videos.

In doing so, the recommendation feature prioritizes the presentation of increasingly more bizarre and dangerous rabbit holes full of extremism, conspiracies[1], and dubious alternate COVID, climate-change, and political facts – content that YouTube has learned keeps users coming back for more.

Similar to Snapchat's decision to create a *Speed Filter*, YouTube chose to create this recommendation feature which they knew, or should have known, was leading to harm.

By focusing on Section 230 immunity from user-generated content, we are overlooking product design decisions which predictably have – as is at issue in *Gonzalez* – allowed, and even encouraged, terrorist groups like ISIS to use YouTube to radicalize, recruit, and glorify global terror attacks.

Reform

During the recent *Gonzalez* oral arguments, Justice Kagan questioned if the Court or Congress should take up Section 230 reform, noting "we are not the nine greatest experts on the internet." In this case, however, the issues do not require deep internet expertise (although I would advise the Justices (and Congress) to become more expert at all things technological).

The technology sector has been highly effective at muddying the waters and scaring the Courts and Congress with the claim that holding platforms responsible for what amounts to a faulty product design would destroy everything on the internet from a Google/Bing search to a Wikipedia page. This is simply untrue and we should not fall for this self-serving fear mongering.

While much of the debate around Section 230 has been highly partisan, it need not be. The core issue is not one of over- or under-moderation, but rather one of faulty and unsafe product design. As we routinely do in the offline world, we can insist that the technology in our pockets are safe. For example, we have done a good job of making sure that the battery powering our device doesn't explode and kill or injure us, but have been negligent in ensuring that the software running on our device is safe.

The core tenants of Section 230 – limited liability for hosting user-generated content – can be protected while insisting, as in *Lemmon v. Snap*, that tech-

[1]M. Faddoul, G. Chaslot, and H. Farid. A Longitudinal Analysis of YouTube's Promotion of Conspiracy Videos. *arXiv*: 2003.03318, 2020.

nology that is now an inextricable part of our lives be designed in a way that is safe.

Summary

When, in 1996, Congress enacted Section 230 as part of the Communications Decency Act, they could not have envisioned today's internet and technology landscape. Congress could not have envisioned the phenomenal integration of our online and offline world, the trillion dollar sector founded on vacuuming up every morsel of our online (and offline) behaviors, and the highly-targeted algorithmic manipulation of nearly everything we see and consume online.

Nearly three decades later, we must rethink the overly broad interpretation of Section 230 that has moved from its original intent of not penalizing Good Samaritans to the current system of rewarding Bad Samaritans. This can be accomplished by clarifying that Section 230 is intended to protect platforms from liability based exclusively on their hosting of user-generated content, and not – as it has been expanded to include – a platform's design features that we now know is leading to significant harms to individuals, societies, and our very democracy.

Senate Committee on the Judiciary Subcommittee on Privacy, Technology, and the Law
Hearing on Platform Accountability: *Gonzalez* and Reform

Testimony of Dr. Mary Anne Franks
Michael R. Klein Distinguished Scholar Chair and Professor of Law, University of Miami
President and Legislative & Tech Policy Director, Cyber Civil Rights Initiative
March 8, 2023

I. Introduction

In the Biblical parable of the Good Samaritan, a traveler is beaten by robbers and left half dead by the side of the road. A priest sees him but passes by without stopping; a Levite later does the same. Finally, a man from Samaria comes upon the injured traveler. He stops, tends to the man's wounds, and takes him to an inn to receive further care. "Good Samaritan" laws, which exist in every state, commonly provide legal protection to individuals who, like the Good Samaritan in the Bible story, voluntarily attempt to assist others in need.

In 1996, Congress passed a "Good Samaritan" law for the internet: Section 230 of the Communications Decency Act. The law's operative provision is titled "Protection for 'Good Samaritan' blocking and screening of offensive material." Legislative headings supply important guidance about a provision's intended meaning, providing "a short-hand reference to the general subject matter" to which Congress meant to apply the provision.[1] Section 230 (c)(2) spells out the significance of the provision's title, expressly offering immunity from civil liability to providers and users of interactive computer services (such as search engines and social media platforms) for actions "voluntarily taken in good faith to restrict access to or availability of" objectionable content.

For more than twenty years, however, most courts have ignored the text and history of Section 230 and instead interpreted this online Good Samaritan law to protect not only Internet sites and services that attempt to restrict harmful content, but also those that make no effort to restrict access to harmful content. Worse still, some courts have even interpreted the law to protect those who *solicit* harmful content, *amplify* it, and even *profit* from it. In this upside-down version of the Good Samaritan parable, not only indifferent priests and Levites, but also enterprising passersby who point crowds to the bloody spectacle for a price, are granted the same protections as the Good Samaritan. In other words, courts have treated Section 230 not as the Good Samaritan law that Congress enacted, but as a Bad Samaritan law that rewards reckless, unaccountable, and destructive online behavior.

The consequences of granting this carte blanche, unqualified immunity to large social media companies and other online platforms are entirely predictable. Harmful content flourishes online, causing grave and lasting injury to vulnerable communities, even when those harms are clearly foreseeable and easily preventable. Sites devoted to nonconsensual pornography, commonly known as "revenge porn," can operate without fear of liability for the devastating social,

[1] Trainmen v. Balt. & Ohio R.R. Co., 331 U.S. 519, 528 (1947).

emotional, and economic harms caused by allowing users to post intimate images of others without their consent. Social media platforms that host forums for the radicalization of bigots and misogynists can avoid any legal responsibility for the online abuse and doxing on their sites directed at vulnerable groups. And the online gathering places for the darkest and most destructive conspiracy mongering enjoy blanket immunity when their sites are used to harass and terrorize election officials or victims of gun violence.

Perpetuating this kind of Bad Samaritan immunity is especially egregious considering how the Internet and social media platforms can exacerbate and magnify the harms of abuse and harassment. The anonymity provided by many social media platforms allows the perpetrators of abuse to avoid detection. The reach and amplification of social media allow abuse to be crowdsourced and broadcast to a wide audience. And the permanence of online content means that harmful content or private information can be nearly impossible to remove from public view. All of this contributes to the virtual captivity in which online abuse permeates every aspect of the victim's life, and opportunities to escape from the global reach of technology are extremely limited. It is therefore no wonder that online abuse has serious consequences for victims' freedom of expression, professional and educational opportunities, civic participation, and mental health.

II. *Gonzalez v. Google* (2023)

On February 21, 2023, the Supreme Court took up the question of the proper scope of Section 230 for the first time. *Gonzalez v. Google* presents the Court with the question of whether Section 230 provides immunity to Google for allegedly using targeted algorithms to promote violent extremist video content. Some critics of the tech industry have argued that the use of targeted algorithms can never be protected by Section 230 immunity, while tech industry supporters claim that the use of targeted algorithms should always warrant Section 230 immunity.

Both of these positions are wrong. Targeted algorithms are one of the most effective tools that online platforms and services can use to restrict harmful content, which is exactly the kind of action that Section 230 immunity is intended to protect. But Google's alleged actions in this particular case *amplified* rather than restricted access to terrorist propaganda. For that reason, the company should not receive Section 230 immunity.

During oral argument in Gonzalez, Justice Ketanji Brown Jackson correctly explained Section 230's text, history, and purpose as a Good Samaritan statute. As such, its primary goal is to incentivize voluntary, good faith interventions against harm. The "unqualified immunity" interpretation of Section 230 erases that incentive to help, and in fact provides an incentive to harm – tech companies can act as recklessly as they want in designing their products and services, because more harmful, provocative content equals more profit.

Defenders of the Section 230 status quo often claim that any restriction in the scope of protection makes online intermediaries legally responsible for everything users post on their platforms. But the absence of immunity is not the same thing as the presence of liability. The bystander who fails to help a robbery victim does not enjoy the benefit of Good Samaritan immunity, but this

does not mean the bystander is legally responsible for the robbery. It is only when and if that bystander not only fails to help, but actively causes harm—for example, by taking photos of the victim to distribute for profit—that they could and should face potential liability for that harm.

A slightly more sophisticated version of this objection maintains that the risk of liability – the mere *possibility* of being sued – will force tech companies to take down any third-party content that could be controversial, resulting in the loss of valuable, First Amendment-protected expression. But as Justice Elena Kagan noted during the *Gonzalez* oral argument, "every other industry has to internalize the costs of its conduct. Why is it that the tech industry gets a pass?" Auto manufacturers can be sued when engines catch on fire; cigarette companies can be sued when smokers get lung cancer; hospitals can be sued for botched surgeries. But cars still get made, cigarettes keep being sold, and doctors still operate. There is no reason to think that allowing people to sue when they are harmed by a product means that the product will cease to exist in any meaningful sense. Indeed, the potential for litigation is often a powerful motivator for industries to become safer, more efficient, and more innovative.

Some argue, however, that the Internet is fundamentally different from cars and cigarettes and hospitals because the product in question is speech, and speech deserves special protection under the First Amendment. It is first important to note that the way that Section 230 is currently interpreted shields far more than speech protected by the First Amendment – everything from defamation to credit card transactions to sales of illegal firearms. People use the Internet for a vast array of activities that are not "speech" in any First Amendment sense: paying bills, selling stolen goods, shopping for dog leashes, booking hotel rooms, renewing driver's licenses. The fact that Section 230 uses the term "information" rather than "speech" has helped tech platforms invoke the law to absolve themselves of responsibility for virtually everything individuals do online – a protection that goes far beyond anything the First Amendment would or should protect.

Second, the tech industry is not the only speech-focused industry. Colleges and universities are very much in the business of speech, but they can be sued for discrimination and harassment. So can book publishers and book distributors, radio stations, newspapers, and television companies. The New York Times and Fox News have no special, sweeping immunity from liability the way the tech industry does; indeed, the *New York Times* was sued just last year by Sarah Palin for defamation and the Fox Corporation is currently being sued for defamation by Dominion Voting Systems. The newspaper and television industries have not collapsed under the weight of potential liability, nor can it plausibly be argued that the potential for liability has constrained them to publishing and broadcasting only anodyne, non-controversial speech.

Of course, some calls for tech industry liability do indeed threaten free speech. Some of the most pernicious attacks on free speech and the First Amendment in recent years have come in the guise of Section 230 reform. While it may be easy to forget, social media platforms are private entities with their own First Amendment rights of speech and association. It is vitally important to respect those rights and to reject any attempt by government actors to force social media platforms to carry certain speech or demand that they provide access to certain speakers. Respecting free speech and the First Amendment means respecting tech companies' right to fact-check, label, remove, ban, and make other interventions as they see fit about the content on their

sites. Providing additional or alternative information to false or misleading posts is classic "counterspeech," a treasured First Amendment value. The First Amendment also protects the right to refuse to host content altogether, as the right to free speech includes both the right to speak and the right *not* to speak. As the Supreme Court held in *West Virginia State Board of Education v. Barnette*, "If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion, or force citizens to confess by word or act their faith therein."[2] The First Amendment also protects the right of association, including the right of private actors to choose with whom they wish to associate.[3] And the Supreme Court has long recognized that private-property owners generally have the right to exclude individuals from their property as they see fit.[4]

But allowing tech companies to enjoy unqualified immunity for everything they promote and profit from inflicts economic, physical, psychological and free speech harms. Those targeted for abuse shut down social media profiles and withdraw from public discourse. Those with political ambitions are deterred from running for office. Journalists refrain from reporting on controversial topics. While the current model shielding the tech industry from liability may ensure free speech for the privileged few, protecting free speech for all requires legal reform.

In deciding *Gonzalez*, the Supreme Court has the opportunity to correct the misreading of Section 230 that has plagued the lower courts for decades and allow it to operate as the kind of Good Samaritan law that Congress originally enacted. If the Court does so, victims of online abuse may finally be able to seek justice against platforms who have contributed to their injuries. And, in turn, platforms may finally recognize the value of taking affirmative measures to curb abuse and protect users.

III. Reform Recommendations

But the Supreme Court may also decide that the task of establishing the proper scope of Section 230 immunity is best left to Congress. As Justice Kagan observed, "we're a court. We really don't know about these things. You know, these are not like the nine greatest experts on the Internet."

If the Supreme Court fails in *Gonzalez v. Google* to scale back the excessively broad interpretation of Section 230 that has taken hold in the courts, Congress should take up the responsibility of amending Section 230 to clarify its purpose and foreclose interpretations that render the statute incoherent. At a minimum, this means two specific changes: amending the statute to make clear that interactive computer service providers that demonstrate deliberate indifference to harmful content are ineligible for immunity; and making clear that the law's protections apply only to speech.

---

2. 319 U.S. 624, 642 (1943).
3. *NAACP v. Alabama ex rel. Patterson,* 357 U.S. 449 (1958).
4. *PruneYard Shopping Ctr. v. Robins,* 447 U.S. 74, 82 (1980).

To accomplish the first change, Section 230 (c)(1) should be amended to state that providers or users of interactive computer services cannot be treated as the publisher or speaker of speech *wholly provided by* another information content provider, *unless such provider or user intentionally encourages, solicits, or generates revenue from the speech, or exhibits deliberate indifference to harm caused by that speech.*

To accomplish the second change, the word "information" in Section 230 (c)(1) should be replaced with the word "speech." This revision would put all parties in a Section 230 case on notice that the classification of the content at issue as protected speech cannot be assumed, but instead must be demonstrated. If a platform cannot make a showing that the content or information at issue is speech, then it should not be able to take advantage of Section 230 immunity.

As important a Section 230 reform is, however, it is not a silver bullet for the wide-ranging harms facilitated by the tech industry. Congress should also enact narrowly targeted federal criminal legislation to address new and highly destructive forms of technology-facilitated abuse, especially those disproportionately targeted at vulnerable groups, including nonconsensual pornography, sexual extortion, doxing, and digital forgeries ("deep fakes"). As Section 230 immunity does not apply to violations of federal criminal law, the creation of these laws will ensure that victims of these abuses will have a path to justice with or without Section 230 reform.

Congress should finally pass the Stopping Harmful Image Exploitation and Limiting Distribution (SHIELD) Act, which would make it a crime to knowingly distribute or threaten to distribute private, sexually explicit visual material of an individual with knowledge of or reckless disregard for the depicted individual's lack of consent to the distribution and reasonable expectation of privacy and without a reasonable belief that distributing the depiction touches a matter of public concern.[5] Congress should also pass a measure similar to the Online Safety Modernization Act of 2017, sponsored by Congresswoman Katherine Clark, which would prohibit multiple forms of "cybercrimes against individuals" including both sextortion and doxing.[6]

Congress should also enact legislation, including criminal legislation, to regulate information that involves verifiably false information that is likely to cause significant harm. Such legislation should include the criminalization of digital forgeries (colloquially known as "deep fakes"). The definition of digital forgeries should be limited to audiovisual material that has been created or materially altered to falsely appear to a reasonable observer to be an actual record of actual speech, conduct, appearance, or absence of an individual, which is created, distributed, or reproduced with the intent to seriously harm or with reckless disregard for whether serious harm

[5] H.R.6998. The SHIELD Act, for which I served as the primary drafter, came very close to becoming law in 2021, when it was included in the House version of the Violence Against Women Reauthorization Act of 2021 but omitted from the Senate version, and again in 2022, when it was included in the omnibus spending bill but removed by Republican leadership at the last moment. *See* Danielle Campoamor, *What it's like to be a victim of 'revenge porn' as a mom: 'It broke my heart,'* Today (Jan. 5, 2023), https://www.today.com/parents/moms/revenge-porn-victims-are-also-moms-speak-rcna62093

[6] H.R.3067.

would result to a falsely depicted individual, or with the intent to incite violence or interfere with official proceedings.

IV. Conclusion

At the most fundamental level, the current problem with the tech industry is the lack of incentive to behave responsibly. The preemptive immunization from liability that courts have interpreted Section 230 to provide means that the drive to create safer or healthier online products and services simply cannot compete with the drive for profit. As long as tech platforms are allowed to enjoy all of the benefits of doing business without any of the burdens, they will continue to move fast and break things, and leave average Americans to pick up the pieces.

The unqualified immunity interpretation of Section 230 creates what economists call a moral hazard: when an entity is motivated to engage in increasingly risky conduct because it does not bear the costs of those risks. The devastating fallout of that moral hazard is all around us: an online ecosystem flooded with lies, extremism, racism, and misogyny that is fueling offline harassment and violence.

Statement of Professor Eric Schnapper

I.

Section 230(c)(1) was adopted for the purpose of distinguishing between conduct of third parties and conduct of internet companies themselves. Its familiar language provides 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." The last four words are central to the limitation on the defense created by the statute; it is only regarding information created by "another" that the defense may be available. Section 230(e)(3) makes clear that even a partial role played by an internet company in the creation of harmful material would fall outside the protections of the statute. Section 230(f)(3) defines the term "information content provider" as "any person or entity that is responsible, in whole or *in part*, for the creation or development of information provide through the Internet or any other interactive computer service."

The legislative history of the statute makes clear that Congress enacted the law because it believed it would be impossible for internet companies to prevent all harmful materials from being posted on their websites, and that it would be unfair to hold them responsible for what was posted there by others, at least if they did not know what was being posted. Representative Lofgren explained the imposing strict liability on an internet company for unknown materials on its website would be "like saying that the mailman is going to be liable when he delivers a plain brown envelope for what is inside it." 141 Cong. Rec. 22046 (1996). Representative Goodlatte made the same point:

> There is no way that any of those entities, like Prodigy, can take the responsibility to edit 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.

141 Cong. Rec. 22046.

Congress acted in reliance on representations that there was no way for internet companies to exhaustively monitor the content of all the material that was being posted. "We have been told it is technologically impossible for interactive service providers to guarantee that no subscriber posts indecent material on their bulletin board services." 141 Cong. Rec. 22046 (remarks of Rep. Goodlatte).

The focus of this concern was expressly restricted to limiting liability for actions by other parties. Thus Representative Goodlatte's comments were about what a "subscriber posts," and about what is "coming in to" internet companies. In Representative Lofgren's hypothetical, the letter carrier was not responsible for whatever someone else had placed in the "plain brown envelope." Both Member of Congress assumed that the role of the internet company would be a limited one; permitting the posting of material "onto [its] bulletin board," or "deliver[ing]" that material to whatever location had been chosen by whoever addressed the envelope.

That account made complete sense in the context of the most common websites of the era when § 230(c)(1) was enacted. The legislative history focused on the three largest websites used by ordinary consumers of that time: Prodigy, CompuServe, and America Online, none of which still exists except in vestigial form. Regarding third-party content, those websites of yesteryear were essentially passive. Users could post material on the websites, or obtain material from it, but the role of the website itself was largely limited to providing structured locations within the website to which materials could be posted or where those materials could be found. Because of the economics of those websites—they charged monthly fees to users—they usually had no interest in increasing the amount of usage by a particular user. In fact, due to limited capacity they were

incentivized to tamp down time spent by users on their sites. Under the monthly fee structure the ideal user was one who utilized the website very little. Indeed, reports from that era were concerned that the increasing use and popularity of websites threatened to overwhelm their technical capacity.

In *Reno v. American Civil Liberties Union,* 521 U.S. 844 (1997), decided shortly after the enactment of § 230(c)(1), the Supreme Court provided a description of the relationship between users and websites in which, with the exception of a search engine, the website itself did nothing at all.

> A user may either type the address of a known page or enter one or more keywords into a commercial "search engine" in an effort to locate sites on a subject of interest. A particular Web page may contain the information sought by the "surfer," or, through its links, it may be an avenue to other documents located anywhere on the Internet. Users generally explore a given Web page, or move to another, by clicking a computer "mouse" on one of the page's icons or links. Access to most Web pages is freely available, but some allow access only to those who have purchased the right from a commercial provider. The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.
>
> From the publishers' point of view, it constitutes a vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and individuals. Publishers may either make their material available to the entire pool of Internet users, or confine access to a selected group, such as those willing to pay for the privilege.

521 U.S. at 852-53 (footnote omitted).

Consistent with the text of the statute, and with its original purpose, courts have repeatedly described the defense created by section 230(c)(1) as inapplicable to conduct engaged in by the website itself.[1]

II.

Within a decade of the enactment of section 230(c)(1), there was a fundamental change in the financial basis of the major consumer website companies, a change which has led those companies to engage in an increasing amount of activity of their own. By the early years of this century, access to the internet was no longer based on subscription-based (and, previously, dial-up) services. Individuals largely accessed the internet through high-speed connections provided cable companies or other local providers. And, critically, the major internet companies that emerged and thrived based their revenues, not on monthly subscriptions, but on advertising.

For an advertisement-revenue-based internet company, the main basis of its income and financial success is the amount of time that users spend on the firm's website; the longer a user is on a website, the more advertisements he or she can be shown, and the more revenue the company will receive. Thus, for these companies, the central task of their business is to find ways to persuade users to spend as much time as possible looking at materials on their websites. Few firms, if any, have been content to hope that third parties will post materials that potential users will find

[1] *Henderson v. Source for Public Data*, 53 F.4th 110, 126 (4th Cir. 2022) ("Public Data's own actions"); *Fair Housing Council of San Fernando Valley v. Roomates.com, LLC*, 521 F.3d 1157, 1169 n. 24 (9th Cir. 2008) ("their own conduct"); *Federal Trade Commission v. LeadClick Media LLC*, 838 F.3d 158, 171 (2d Cir. 2016) ("LeadClick's own actions"); *Lemon v. Snap, Inc*., 995 F.3d 1085, 1093 (9th Cir. 2021) ("its own conduct") (quoting *Maynard v. Snapchat, Inc*., 346 Ga. App. 131, 816 SE 2d 77, 81 (2018)); *Webber v. Armslist LLC*, 572 F. Supp. 3d 603, 616 (E.D. Wisc. 2021) ("their own misconduct"); *Lee v. Amazon.com, Inc*., 76 Cal. App. 5th 200, 257, 291 Cal. Rptr. 322, 377 (Ct. App. 1st Dist. 2022) ("Amazon's own conduct"); *Massachusetts Port Authority v. Turo, Inc*., 487 Mass. 235, 243 (2021) ("Turo's own conduct").

interesting, or to simply wait until users at their own initiative ask to see a particular video, tweet, or text. Rather, the focus of much of the activity of most advertisement-revenue-based websites is to devise automated strategies of their own—typically relying on algorithms—to promote and increase such usage.

Targeting using algorithms has been central to these promotional efforts of websites. Most websites have a wide variety of users. Efforts to promote the same third-party content to all users would often be ineffective; a prominently displayed thumbnail about a cooking video on YouTube's home page would be unlikely to interest users primarily concerned with sports, pets, current events, travel, fashion, or archeological discoveries. Instead, major websites collect copious amounts of data about users, and rely on what they know about each user, including information about which materials he or she has viewed in the past, how long was spent viewing it, how often a particular user follows up with more videos on similar subjects, etc., to select the particular material to recommend. Working in the background, the internet company's algorithm develops an ever-more-detailed, and constantly updated and pruned, profile of each user. The algorithms are constantly being tweaked to result in longer viewer engagement by targeted users; some of those ongoing adjustments are made directly by software engineers, and some by artificial intelligence software which monitors the ways in which users have responded to past recommendations.

Most Americans have experienced the effectiveness of these algorithms in the context of promoting advertising. As one uses a website like YouTube, Facebook, TikTok, etc., those sites show the Used in this manner, the algorithms allow advertisers to laser-focus their advertisements on particular micro-demographics. This can also create problems, such as when a housing

developer focuses real estate listings on a demographic profile that excludes particular racial groups.

The internet companies use similar algorithms to induce users to remain on their websites longer so they will view more of these targeted advertisements. The manner in which websites seek to induce users to look at particular materials, and to remain on the website (and available for advertising) for as long as possible, vary widely, and are continuing to evolve. Officials in these companies generally refer to these practices as "recommendations," although that is not a term in § 230(c)(1) itself and has no fixed meaning in either the law or in industry usage. Today those promotional practices, taken at the initiative of the website itself, rather than in response to some request from a user, include the following:

> *Displaying unrequested videos, pictures or text*—Once a user looks at a particular item, or selects a type of material, the website displays a continuous series of materials, materials generally chosen by the website's algorithm to maximize the likelihood that the user will continue to watch whatever the website has selected. Autoplay in YouTube is such a feature, and much of what occurs on TikTok and Instagram functions that way.
>
> *Displaying advertisements for promoted material*—Websites may proffer to a user what are in effect a targeted set of advertisements for material available on the website itself. The thumbnails that a user sees on YouTube are usually chosen in that manner, as are the snippets of text that appear on Feed (formerly News Feed) on Facebook. A URL (usually created by the website itself) is embedded in each thumbnail or snippet, so that a user can easily access the promoted material. On Facebook pictures of possible new individuals to "friend" function in this manner.

Promotional language—Websites sometimes include words or information of their own to encourage users to select particular materials, terms such as "trending," or "you might like," or data about the number of likes or views.

Notifications—Websites may send push notifications, text messages or emails to viewers announcing newly available materials, or post such announcements on a page a user will visit.

Autocomplete—TikTok includes a feature that tends to direct users to particular content by automatically completing search terms as the user starts to type them. According to a complaint recently filed by the Indiana Attorney General, that feature often directs users to materials about drugs and sexual materials inappropriate for minors. The complaint alleges, or example, if a user types "shr" into the TikTok search bar, TikTok suggests "shroomz" as a possible search term, which leads the viewer to materials about hallucinogenic mushrooms.

These various website promotional practices have, overall, been extremely effective. YouTube officials, for example, estimate that about 70% of the views on its website are a result of its recommendations.[2]

III.

Although these promotional practices have been quite lucrative, they also have resulted in streams of increasingly harmful materials being directed at users. Evaluations of the distribution

[2] YouTube's Recommendations Drive 70% of What We Watch," available at qz.com/1178125/youtubes-recommendations-drive-70- of-what-we-watch, visited Nov. 16, 2022.

of terrorist and other extremist materials have concluded that most of those distributions is a result of website algorithm-based targeted promotional practices.

In 2019-20, a researcher employed by Facebook created an account for a fictional user named Carol Smith. The fictional Smith described herself as a politically conservative mother from North Carolina, with an interest in politics, Fox News, and then-President Trump. Although that description did not express an interest in conspiracy theories, within two days the Facebook algorithms were recommending that she join groups dedicated to QAnon. Within a week, Smith's feed was full of groups and pages that violated Facebook's nominal rules, including those against hate speech. That study, entitled "Carols's Journey to QAnon," and other Facebook studies that showed test users receiving a "barrage of extreme, conspiratorial and graphic content," have ben provided to Congress in redacted form by Frances Haugen.

In 2022 a study of YouTube yielded a similar result. An Arabic language search for the term "Jews" and for the name of a Hamas official soon led to videos lauding suicide bombings, and containing antisemitic rhetoric about the Rothschild family.[3]

A number of analyses have suggested that this occurs because website algorithms have concluded that exposing users to more extreme content is likely to result in longer periods of viewing of the website in question. The large amount of information that websites often have about individual users makes these practices especially effective in radicalizing users and recruiting terrorists. If YouTube posted ISIS recruiting videos on a website shown to everyone who visited YouTube, the overwhelming majority of viewers would simply be horrified. But YouTube has,

[3] Brief of Amici Curiae Major General Tamir Hayman, *et al*., Gonzalez v. Google LLC, No. 21-1333, at 27-28

and uses, the ability to identify and target the particular individuals likely to watch terrorist or extremist videos, an ability which the terrorist or domestic extremist groups themselves lack.

When websites first began to engage in promotional practices, they could have chosen to limit such recommendations to a carefully screened group of videos, texts, and tweets. Or, recognizing that this use of recommendations bears no relationship to the passive role that § 230(c)(1) was adopted to protect, internet firms could have asked that Congress to amend the statute. Instead, those firms simply swept into their recommendation functions whatever was on their websites. Thus the affirmative promotion of terrorist or other extremist material has followed inexorably from the failure of websites to identify and remove those materials in the first place.

The consequences of these practices for national security have been exceptionally serious. In the *Twitter, Inc. v. Taamneh* litigation, a group of retired United States generals, including first commander of Operation Inherent Resolve in Iraq and Syria, explained that:

> social media played a central role in making [ISIS], at least for several years, the most successful and most viscous terrorist group in modern history,… ISIS['s]…massive recruitment effort, carried out to a significant degree through the [Twitter, Facebook and YouTube]'s social media platforms, is one key to ISIS's initial success.[4]

Other Defense Department officials pointed out that:

> ISIS has used [social media] platforms to exhibit intimidation, networking, recruitment, justice, and justification…. The group has embraced social media as a weapon of war, using it to spread official messages, recruit, fundraise, and network.[5]

---

[4] Brief of Amici Curiae Retired United States Generals, *Twitter, Inc. v. Taamneh*, 3-4 (emphasis omitted).

[5] Heather Marie Vitale and James M. Keagle, "A Time to Tweet, as Well as a Time to Kill: ISIS's Projection of Power in Iraq and Syria, Defense Horizons," Nat'l Defense Univ. 1, 6 (Oct. 2014).

While this subcommittee meets to discuss website promotional practices, several thousand members of the United States armed forces remain in harm's way on the ground in Syria and Iraq dealing with the consequences of those actions.

For decades social media platforms have steadily become overrun with hate speech, incitement to terrorism, domestic violence, and calls for antisemitic violence. The refusal of social media platforms to implement effective steps of self-regulation have resulted in the murder of Nohemi Gonzalez, Mehier Taamneh, and many other innocent victims worldwide. While the social media platforms have to flourished and prospered, the safety of the American public and other communities worldwide has been imperiled as terrorists are provided use of this powerful tool to carry out their deadly attacks. Congress never intended section 230 to provide a defense for internet companies when their own conduct causes such grievous harms.

In August and September 2014, American journalists James Foley and Steven Soloff were beheaded by ISIS, horrific events videotaped and publicized by their killers. Two months later, a spokesman for Twitter, in explaining why Twitter still was not removing ISIS from its platform, explained "[o]ne man's terrorist is another man's freedom fighter."[6] Those extraordinary eight words are a compelling demonstration that absolute immunity can breed absolute irresponsibility. This subcommittee will doubtless be assured that that attitude has changed. But as recent events have made all too clear, in the absence of any legal consequences for policies based on that attitude, and as long as websites can wield § 230(c)(1) like a human shield to protect their own conduct, any existing website policy could be swept away with the next change in ownership or personnel.

[6] Jenna McLaughlin, "Twitter Is Not at War With ISIS. Here's Why," MOTHER JONES (Nov. 18, 2014).

STATEMENT OF

ANDREW SULLIVAN[1]
PRESIDENT AND CHIEF EXECUTIVE OFFICER
INTERNET SOCIETY

BEFORE THE
SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW
OF THE COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED
"PLATFORM ACCOUNTABILITY: GONZALEZ AND REFORM"

PRESENTED MARCH 8, 2023

Good afternoon, Chair Blumenthal, Ranking Member Hawley, and distinguished members of this Subcommittee. Thank you for the opportunity to appear before you today to discuss platform accountability.

Founded in 1992, the Internet Society is a U.S. non-profit organization headquartered in Reston, Virginia, and Geneva, Switzerland, with a core mission of promoting and defending the Internet. The Internet Society's staff comprises technical experts in internetworking, cybersecurity, and network operations, among other fields, as well as policy experts in a broad range of Internet-related areas.

A key characteristic of the Internet—one that sets it apart from every other communications media—is that it was meant to be open for everyone. Individuals can speak, debate, create, invent, and engage with others, whether they are across town or around the world. The broad protections that Section 230 affords are essential for—in the words of that statute—this "interactivity" on the Internet. Simply stated, without the basic protections that Section 230 provides, we would not have the robust engagement of hundreds of millions of Americans in the online conversation, nor would we have the astounding innovation in online services that we have witnessed over the past 25 years.

It is certainly true that as more of our society's discourse has moved online, so have a number of serious societal problems. We appreciate that Congress is looking to address some of those problems. Americans are, quite reasonably, concerned that speech and behavior that would not be tolerated in other settings are seemingly not only protected, but even exploited for profit,

[1] I wish to express thanks to my colleagues at the Internet Society, and especially to John Morris, in the preparation of this testimony.

in some online platforms. At the same time, the power of those very platforms appears only to grow, such that they have outsized influence and power in the social and political life of the nation and other nations around the world. Yet it is important not to lose sight of the value of the Internet. For every appalling example of childhood sexual abuse material, there is an example of a young person who was in crisis and found online a community of others like themselves. Examples of nasty online speech abound, but so do examples of people reaching out and giving one another support in times of need. Some consumers of content on platforms appear to see only polarizing influences; but plenty of others seem to use the same platforms for education, and thereby to better themselves. The Internet can be a conduit for social problems, yes, but it is also an enormous resource for social good. Any changes to the rules about its operation must be undertaken with enormous care.

Our core message to this Subcommittee is that—because of its critical role in ensuring the very ability of individuals to speak online—Section 230 is not the appropriate vehicle through which to try to address social problems. Amendments to Section 230 risk the viability of what makes the Internet unique—the ability of individuals to participate in the global marketplace of ideas.

To appreciate these risks, we must all remember why Congress took the bold steps to create Section 230 in the first place. It was a very early stage of development of the public Internet—and the legal landscape that applied to it—that Congress confronted when it enacted what became Section 230. But in its wisdom, Congress created the broad scope of protections that Section 230 affords far beyond the major online platforms that have since emerged. As a result, there are serious risks that would flow from removing those protections. We address each of these points below, as well as discussing the Gonzalez case, referenced in the title of this hearing.

A. THE ORIGINS AND GOALS OF SECTION 230

The Internet was developed in the 1970s (by a number of the founders of the Internet Society, among others) within the U.S. academic community through a federal government project.[2] Even at this early stage, the potential for interactivity—individual participation—unique to the Internet was plain. In the 1970s and 1980s, it was used primarily for collaboration between academic, government, and commercial researchers, with non-research commercial traffic effectively prohibited. The broad ban on commercial activity—including commercial services offered to individuals—lasted until the Internet was transitioned to the private sector, in April 1995, about nine months before Section 230 was enacted.[3]

The Internet's design is somewhat peculiar in that it is not a single system, but rather a system built up from other systems. This nature is immediately apparent from its name—the Inter-net. The designers recognized that the best way to deploy a very large, distributed network

[2] Vint Cerf, *A Brief History of the Internet and Related Networks*, Internet Society, https://www.internetsociety.org/internet/history-internet/brief-history-internet-related-networks/.
[3] *See A Brief History of NSF and the Internet*, National Science Foundation (Aug. 13, 2003), https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050.

was to take advantage of various other, existing networks, and link them together with some basic common technology. This fundamental design of the Internet is what has allowed it to grow so large. As new needs, areas of operation, or inventions come along, new networks can join the Internet without adjusting the rest of the system. This feature of the design is especially relevant for any consideration of changes to Section 230, because it creates many different actors whose actions might be implicated in any liability question.

Over the 1970s and 1980s, privately-operated networks were also created, ranging from commercial-focused communications networks to "bulletin board" services for individuals or small groups to communicate. As early as 1992, the Hartford Courant reported that "computers [are] growing as [a] forum for ideas"—the newspaper reported on a political debate through a bulletin board involving individuals in Wethersfield, CT, St. Louis, MO, and Glendale, AZ.[4] One of the earliest successful private networks—CompuServe—was founded in 1969 as a "dial up" network aimed at businesses, before later offering its services to individuals, who were then able to engage, share content, and collaborate with people far beyond their local communities. As restrictions on commercial traffic on the Internet eased, these other networks also had the opportunity to join the Internet, bringing even more people into one global online community even as they continued to receive service from their preferred service provider.

As with all forms of communication since the emergence of the common law, there arose the question of how liability for harmful or illegal content would be assigned in the online context. With "first-party" speech—where the speaker and the platform for speech are the same entity—liability was always clear: the first-party speaker would be liable. What was unclear was responsibility for "third-party" speech—speech by speakers that was carried or conveyed by others. Throughout the history of this country, the rules for responsibility for third-party speech under the common law have appropriately varied by the medium of the speech:

- **Broadsheets, pamphlets, and speech on the village green:** Generally, there was no third-party speech involved, and thus only first-party liability applied.
- **Newspapers:** Most speech is first-party speech, but the newspapers can be liable for third-party speech (such as letters to the editor).
- **Telephones:** Under the common carriage regime, telephone companies were not liable for speech made over their networks.
- **Radio and broadcast television:** Similar to newspapers, with potential liability for the broadcaster if they carry third-party speech.
- **Cable television:** Through private negotiations between the cable channels and cable systems, liability was allocated to the cable channels.

But the Internet is fundamentally different than any of those media, with literally orders of magnitude more people and entities involved in the liability questions. In the 1990s, two

[4] Hartford Courant, Computers Growing as Forum for Ideas, Aug. 17, 1992 (available at https://www.courant.com/1992/08/17/computers-growing-as-forum-for-ideas/). The article identified one Connecticut political observer who saw "the beginning of a vast change in how people learn about and discuss politics," quoting him as saying: "There are 65 million computer users in the United States, and they're just starting to use their modems."

seminal cases began to answer the question of whether online service providers would be liable for content posted by individual users. *Cubby, Inc.* held that an online service provider would not be held liable for speech made by a participant in an online forum, but *only* because the provider had not moderated any content. *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991). Then *Stratton Oakmont, Inc.* held an online service provider liable for participants' speech because the provider engaged in some content monitoring and regulation. See *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). These cases created significant uncertainty and potentially crippling liability for the developing industry of online service providers, including companies that facilitated access to the Internet and third-party speech.

It is against this backdrop that Congress considered and enacted the "Internet Freedom and Family Empowerment Act," which became 47 U.S.C. Section 230.[5] One of Congress's explicit goals for Section 230 was "to promote the continued development of the Internet and other interactive computer services and other interactive media." 47 U.S.C. 230(b)(1). Congress recognized that interactive computer services in general, and the Internet in particular—even at its early stage when Section 230 was enacted—offered what was at the time a profoundly unique platform for interactive communication. Congress observed in the statute that the "Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." *Id.* 230 (a)(3). In Congress's judgment in 1995, these interactive communications, which foster public discourse, should be encouraged. The Internet, unlike prior "published" forms of mass communication, transforms the individual from a passive recipient of mainly corporate-created products into an active participant in shaping communication and content. Congress recognized that this individual-driven "interactivity" was an essential attribute of the emerging Internet that warranted protection.

The results of the Congressional foresight to enable citizen speech and innovation are undeniable. A vast amount of communication (artistic, political, intellectual, pedestrian, and otherwise) now flows through the Internet—whether through blogs, message boards, social media both large and small, videos or music uploaded to the Internet, or other means. Already by 1997, the U.S. Supreme Court noted in its *Reno* decision the "dramatic expansion of this new marketplace of ideas," and the Court held that speech on the Internet warrants the highest level

[5] The "Internet Freedom and Family Empowerment Act" passed by the U.S. House of Representatives in part as an alternative to the "Communications Decency Act" (CDA), which was proposed and passed by the United States Senate. A joint Senate-House conference committee decided to include both the CDA and House-passed Section 230 in the Telecommunications Act of 1996. CDA's rules on "indecent" and "patently offensive" content were quickly challenged and subsequently struck down on First Amendment grounds by the United State Supreme Court in Reno v. ACLU, 521 U.S. 844 (1997), but Section 230 had not been challenged and was not at issue in the Reno decision. *See* Ashley Johnson & Daniel Castro, *Overview of Section 230: What It Is, Why It Was Created, and What It Has Achieved*, ITIF (Feb. 22, 2021), https://itif.org/publications/ 2021/02/22/overview-section-230-what-it-why-it-was-created-and-what-it-has-achieved.

of Constitutional protection under the First Amendment.[6] The lower court in that case had observed the beneficial "democratizing" effects of Internet interactivity, and noted "that the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country—and indeed the world—has yet seen."[7]

B. THE BROAD SCOPE OF SECTION 230 PROTECTIONS

As this Subcommittee considers "platform accountability," it is vital that it understand that Section 230 protects providers and individuals far, far beyond the major online content platforms. Section 230 is applicable—and needed—at almost every level and in every corner of the Internet ecosystem.

Foremost—and often overlooked in discussions of Section 230—is that it directly and critically protects hundreds of millions of Internet users in America. In addition to companies and organizations that offer Internet and online services, Section 230 also specifically protects "users" of those services. Thus, every time that an American re-tweets a humorous or outrageous tweet, they are protected by Section 230 in the event that the original tweet is found to be defamatory or otherwise harmful. Similarly, every time an American on social media forwards an interesting newspaper article or a hard-hitting online restaurant review, they are protected by Section 230 from liability for the underlying content.

Beyond this type of common user engagement that is protected by Section 230, individual Americans—as well as many community groups, political organizations, and local governmental agencies—are protected by Section 230 when they host discussion forums online that allow other people to discuss a topic. Here are just a few examples of the thousands—if not hundreds of thousands—online discussion fora:

- The "Bethel, CT Forum" is a "forum of local political discussion with bipartisan views," with more than 8,000 members, at https://www.facebook.com/groups/615946511795955;
- a subreddit hosts discussions focused on New Haven, CT, at https://www.reddit.com/r/newhaven/;
- a Missouri-based blogger hosts comments and discussion at https://blogodidact.blogspot.com;
- "Lathrop Missouri Discussion" is a discussion group focused on any "concerns, problems, ideas, … Lathrop business or events," at https://www.facebook.com/groups/1690547144552949/about;
- the Missouri Department of Health and Senior Services hosts a private discussion group, limited to public health nurses, named the "Missouri Public Health Nursing Discussion Group," at https://health.mo.gov/living/lpha/phnursing/pdf/discussion-group.pdf;
- "Southeast Missouri political discussions" is a private discussion group with 701 members, at https://www.facebook.com/groups/2731558740434487/.

---

[6] *Reno v. American Civil Liberties Union*, 521 U.S. 844, 885 (1997).
[7] *Am. Civil Liberties Union v. Reno*, 929 F. Supp. 824, 881 (E.D. Pa. 1996).

As may be obvious, there is a huge diversity of online discussion groups in every state across the country, most of which are hosted by individuals, small organizations, government agencies, and others. And of course there is a vast array of national discussion fora, ranging from https://liberalforum.net to https://conservativepoliticalforum.com, and from https://www.reddit.com/r/Cooking/ to https://www.gardenstew.com/, and from https://racing-forums.com/forums/nascar-chat.8/ to https://www.reddit.com/r/rugbyunion/. Every person and organization hosting or moderating those discussion groups is directly protected by Section 230 for liability for content posted in their fora by other people.

Beyond the non-commercial sites identified above, many commercial entities also host comments from customers, users of their products, and people interested in their work. Some small online retailers allow customers to post reviews of their products, some newspapers (such as the https://www.emissourian.com/) allow readers to post comments, and there are numerous software and service providers aimed at enabling small businesses to build interactive online communities of their customers. Any of these small businesses that allow customers, users, or the public to post comments are directly protected by Section 230.

In addition to the participation of individuals and small organizations on the Internet, of great concern to our organization is that Section 230 also protects many different types of service and infrastructure providers in the Internet ecosystem. Those providers include (but are not limited to):

- Internet Service Providers ("ISPs"), who make it possible for individuals to access the Internet. Whether through cable, digital subscriber lines, fiber, wireless, or satellite connections, ISPs enable Internet access. Section 230 ensures that ISPs are not responsible for regulation and monitoring of third-party content transmitted over these services. And according to BroadbandNow, in the United States there are "more than 2,846 Internet service providers, with most covering very small areas." This includes, for example, 82 ISPs in Connecticut, and 278 in Missouri.[8]
- Content Delivery Networks (CDNs), which are specialized network providers, also depend on Section 230 immunity. CDNs are geographically distributed networks of proxy servers and data centers, and they are crucial to delivering large amounts of data (such as delivering high-definition streaming video) quickly to many viewers simultaneously.
- Web hosting companies, many of which, around the country, specialize in helping local small businesses get online. Section 230 is critical to their existence.

Each of these types of infrastructure providers—and others—depends on Section 230 to enable them to efficiently convey traffic to the final destination without risk of liability or obligation to screen content passing through their networks. That includes operators of systems—such as ISPs or voice-over-IP providers—that have no involvement at all with the content that passes through their systems. Like the individuals discussed earlier, their ability to fully participate in the online ecosystem is heavily dependent on the continued protections under Section 230.

[8] *See* https://broadbandnow.com/Missouri and https://broadbandnow.com/Connecticut.

C. SERIOUS RISKS FROM REDUCING SECTION 230 PROTECTIONS

A complete repeal of Section 230 would be immediately catastrophic to the Internet, the hundreds of millions of Americans who use and engage online over the Internet, and the tens- or hundreds-of-thousands of businesses in this country that directly offer Internet-based services. The thousands of very small Internet Service Providers—which provide Internet access to many thousands of small, rural, and underserved communities across this country—would immediately be at grave risk of being sued for harmful content transmitted over their networks. And even if they might ultimately prevail in such lawsuits, the costs of litigating can be crushing and could easily put them out of business. Many more thousands of other businesses would similarly face grave risk for providing online services. And over time, as the understanding of the risks became clearer, many businesses would simply choose to shut down. Only the very largest players in the various markets—ISPs, web hosting providers, online platforms—could safely be predicted to survive.

But an even graver risk is that Congress will consider and enact a more limited "reform" of Section 230 that—as a practical matter for individuals and small businesses—would have the same basic effect of a total repeal. Amendments that carve out new exceptions or add new limitations to Section 230 could easily create too much risk of liability for individuals and small businesses. Although this hearing is about "platform accountability," the vast majority of the individuals and entities protected by Section 230 do not even remotely have access to the resources—or lawyers—that are available to the major online platforms. Many if not most businesses in America would be severely threatened by facing even a single serious lawsuit (especially one that cannot be quickly dismissed as Section 230 permits), and an increase in litigation risk for online speech would drive some companies out of businesses, and would certainly discourage other potential start-ups from entering the field at all.

These risks of liability would profoundly damage the ability of users to speak and receive information online. Providers facing the risk of crippling liability would rationally decide not to carry user or other third-party speech at all, or to carry only a very limited amount that it could be confident would not subject it to liability (e.g., because it was entirely non-controversial or came from an "authoritative" source). In other words, repealing or substantially limiting Section 230 would reduce the opportunity for users of all stripes to engage in speech online.

The reason for this danger goes back to the very nature of the Internet itself. Because it is a distributed network of other networks, there is no central point of control, and a huge abundance of parties involved in its operation. Many of the proposals one hears to address the societal problems the United States faces are, really, efforts to address the behaviors of small handfuls of organizations involved in the operation of the Internet, or even merely services that depend on the Internet. But any changes to Section 230 risk involving all of those other organizations that make the Internet such a resource for all humanity. That is why it is so important to recognize why Section 230 covers so much: it must, because the diversity of people involved in making the Internet is so large.

Because Section 230 protects the entire Internet ecosystem—and the very ability of individuals to participate online—it is a very poor vehicle through which to seek to address problems caused by a small subset of bad actors, actors who may or may not be covered by Section 230. This is not to say that Congress is powerless to address important social problems. Approaches that give rights to all Americans—such as baseline privacy legislation—would be an important start to address some of the current lack of protections in the online sphere. More direct regulation of certain categories of online services could also be appropriate in some cases.[9] And, although we have not seen any examples proposed to date, we do not reject the logical possibility that a focused amendment to Section 230 might achieve socially desirable goals without gravely undercutting the Internet. The Internet Society certainly stands willing to consult and provide feedback on any proposals to address social problems online.

D. GONZALEZ V. GOOGLE LLC

As we argued in our amicus brief in support of affirmance,[10] we believe that the lower courts in that case reached the correct result under both the statutory text and the Congressional intent of Section 230. It is clear that the *Gonzalez* case—although tragic—is covered by Section 230, and the intermediary involved should not be liable for the content of the videos at issue.

In *Gonzalez*, the plaintiffs/petitioners raised two particular arguments that warrant discussion. First, they asserted that the protections of Section 230 should be deemed to be limited to "traditional editorial functions"—a term or concept not found in the statutory language of Section 230. As our brief describes in detail, far from seeking to enshrine some notion of "traditional" editorial functions, Congress was expressly seeking to protect content management tools and techniques that were—as Congress put it—"rapidly developing." 47 U.S.C. 230(a)(1). In seeking to protect innovation, Congress expressly anticipated that many "editorial functions"—including "filter[ing], screen[ing], allow[ing], … disallow[ing,] … choos[ing] … organiz[ing], reorgan[izing] or translat[ing] content"—would be performed by computer software, not by humans. See 47 U.S.C. 230(c)(2)(B), (f)(4). There is no support in the statutory language that Section 230 only protects "traditional editorial functions."

Second, the plaintiffs/petitioners asserted that the fact that the video platform used a general purpose "algorithm" to offer to users new videos to watch based on prior videos the user had watched somehow took the case outside of Section 230. Yet, as suggested by the statutory language quoted immediately above, Congress specifically understood that humans could not possibly moderate or organize all of the content coming online, and thus Congress afforded protection for modern non-human techniques to organize and present content. Moreover, any

---

[9] It is also true that *any* new U.S. law responding to categories of speech online—whether altering Section 230 or not—will face significant constitutional hurdles. The vast majority of speech online—even some harmful or unwanted speech—is lawful under the First Amendment. Private companies that offer Internet-based services themselves have First Amendment rights to carry—or not carry—any lawful speech.

[10] Available at https://www.internetsociety.org/wp-content/uploads/2023/01/Internet-Society-Gonzalez-v-Google-Amicus-Brief.pdf.

organization of content—even alphabetical order[11]—utilizes one or more algorithms. There is no support for the contention that the use of an algorithm somehow takes the actions of an intermediary outside of the coverage of Section 230.

CONCLUSION

Online content can raise difficult concerns—concerns appropriate for Congress to consider addressing. But any action by Congress should not come at the cost of the enormous positive benefits that have flowed, and continue to flow, from the fact that hundreds of millions of Americans are able to go online and express their opinions, share their creative works, pursue innovative and sometimes lucrative new ideas, and generally engage in the global online conversation.

We appreciate the opportunity to testify to this Subcommittee, and we welcome any questions you may have.

[11] *See, e.g.*, *Let's Learn Algorithms: Sorting a list of strings in alphabetical order with bubble sort*, undated, available at https://www.calhoun.io/lets-learn-algorithms-sorting-a-list-of-strings-in-alphabetical-order-with-bubble-sort/; *Sorting Algorithms*, undated, available at https://brilliant.org/wiki/sorting-algorithms/.

Senator Dick Durbin
Chair, Senate Judiciary Committee
Written Questions for Hany Farid
Professor, School of Information and Electrical Engineering and Computer Science, University of California, Berkley
March 15, 2023

1. In your testimony, you described five years of "asking, begging, pleading with the tech companies" to do something about child sexual abuse material on their platforms. You also said that "they came kicking and screaming to do that absolute bare minimum and they have been dragging their feet for the last ten years as well."

   a. **Please elaborate on your view of the commitment of tech companies, including social media and app stores, to address online child sexual exploitation. What more could they be doing?**

   b. **From your perspective, why is child safety not taken more seriously by the tech industry, including social media and app stores?**

2. In response to comments about differences in resources across companies in the tech industry to respond to legal challenges, you said that "small companies have small problems."

   In your view, why should differences in legal resources across companies not be a barrier to Section 230 reform?

Questions for the Record from Senator Alex Padilla
Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law
"Platform Accountability: Gonzalez and Reform"
March 8, 2023

Questions for Mr. Andrew Sullivan

1. How does Section 230 enable online interactivity?

2. During the hearing as well as during the Supreme Court oral argument in *Google v. Gonzalez*, some argued that simply because a company may not have immunity from suit for a particular piece of content it chooses to host, does not mean that it can be found liable for that content. In other words, lack of immunity does not automatically mean liability, which should minimize concerns about limiting the scope of Section 230 protection either via statutory interpretation or legislative amendment. **What are your thoughts on this line of argument?**

3. As the title of the hearing properly alludes to, there's a lot of Congressional and public interest in ensuring that we have a legal and regulatory environment that enables consumers and regulators to hold companies accountable for their own harmful conduct.

    a. **Under existing Section 230 caselaw such as the 2008 Ninth Circuit decision in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC* and recent Fourth Circuit decision in *Tyrone Henderson, Sr. v. The Source for Public Data, L.P.*, how can platforms be held accountable for their own conduct?**

    b. **What tools are available to consumers and regulators to hold platforms accountable for their own harmful conduct?**

4. In her testimony Professor Franks suggests that we consider amending Section 230 to limit the scope of the provision to speech as opposed to "information" by replacing the word "information" in Section 230(c)(1) with "speech." **What are your thoughts on this proposal?**

5. Congressional debates about intermediary liability reform are usually rhetorically limited to those actors that operate at application layer of the Internet. However, as you shared in your testimony, Section 230 extends to the infrastructure intermediaries below them. You highlighted in particular: Internet Service Providers, Content Delivery Networks and Web Hosting Companies.

a. What should legislators know about the different kinds of intermediaries protected by Section 230?

b. How should these differences inform proposals to amend Section 230?

74

Senate Judiciary
Platform Accountability: Gonzalez and Reform

Hany Farid, Ph.D.

Questions

Q1. In your testimony, you described five years of "asking, begging, pleading with the tech companies" to do something about child sexual abuse material on their platforms. You also said that "they came kicking and screaming to do that absolute bare minimum and they have been dragging their feet for the last ten years as well. Please elaborate on your view of the commitment of tech companies, including social media and app stores, to address online child sexual exploitation. What more could they be doing?

Even in the early days of the web, it was clear that services provided by technology companies were being used to spread child sexual abuse material (CSAM). As early as 1995, the chatrooms of AOL – an early incarnation of today's social media – were allegedly used to share CSAM. In response, AOL executives at the time claimed that they were doing their best to rein in abuses on their system but that their system was too large to manage. This is precisely the same excuse that we hear nearly three decades later from the titans of tech.

By early 2000, there was an explosion of CSAM online. Between 2003 and 2008, despite repeated promises to act, major tech companies failed to develop or deploy technology that could find and remove CSAM. Then in 2009, I partnered with Microsoft to develop the technology photoDNA which quickly and accurately finds and removes known instances of CSAM as it is uploaded. PhotoDNA is provided at no cost to technology companies. Despite being free and easy to deploy, it took years of pressure, begging, and pleading, for photoDNA to be adopted by many (but not all) web services and networks.

In under a year, a small team of us developed, tested, and deployed photoDNA. How could it possibly be that over a five-year period the top technology

companies could not do this? The issue was never one of technological limitations. It was a matter of will and moral bankruptcy – the technology companies simply did not want a solution and so they did not find one.

Since the release of photoDNA in 2009, technology companies have individually and collectively failed to further innovate to respond to an increasingly sophisticated criminal underworld. For example, despite foreseeing the rise in child-abuse videos, tech firms have not yet deployed industry-wide systems that can identify offending footage like photoDNA can do for images. Despite the use of live-streaming services to broadcast the sexual abuse of children, the industry has done nothing to prevent this abuse. Despite knowing that their services connect children with predators, the industry has done virtually nothing to prevent this abuse, and have in fact continued to design their services to enable and even encourage these dangerous interactions. And, even when notified of CSAM on their services, some like Twitter and Google are maddeningly slow at responding.

Developing technology to address these harms is possible. The technology sector as a whole simply does not prioritize protecting children online. Instead, they seem only interested in harvesting the data of children and – like the tobacco industry – addicting increasingly younger children to their services.

Q2. From your perspective, why is child safety not taken more seriously by the tech industry, including social media and app stores?

Unlike the music and movie industry that lobbied to pass the DMCA to protect their financial interests, victims of child sexual abuse do not have a powerful lobby. As a side note, what does it say about a society that protects the interests of a billion-dollar industry before it protects their children?

The longer – less flippant – answer is that social media profits from user-generated content. Moderating content and taking down content is simply bad for business. In addition, if platforms developed and deployed effective content to remove CSAM, then they would have no excuse to not remove other harmful, illegal, or violative content. That is, an effective response to removing CSAM opens the door to reining in other forms of problematic (and profitable) content. Without the proper external pressure, the industry will simply not choose to act against their financial interests.

Q3. In response to comments about differences in resources across companies in the tech industry to respond to legal challenges, you said that "small companies have small problems." In your view, why

should differences in legal resources across companies not be a barrier to Section 230 reform?

When the DMCA was passed, the large technology companies made the same claim that managing DMCA take-down requests would cripple small platforms. It did not.

In 2018 the German NetzDG law went into effect requiring online platforms to quickly respond to reports of hate speech and illegal content. Large tech companies claimed that this would hurt smaller platforms and force all platforms to over-moderate – the same claims being made today around discussions of 230 reform. Neither prediction came true. Since its adoption, there has been no evidence of over-moderation or burdensome compliance costs[1].

Despite the lack of evidence to support claims that regulation will cripple innovation and smaller services, safeguards can be put in place. The European DSA, for example, distinguishes between "very large online platforms" (defined as platforms reaching 45 million average monthly users or more) and mid- and small-size platforms. The law places different rules and penalties based on platform size and reach with the very larger platforms being held to a higher standard.

The titans of tech are simply using scare tactics to avoid responsibility. We should, of course, be thoughtful on how any regulation will impact innovation, but as we saw with the automotive industry, safety need not be pitted against innovation and profits – safer products are good for everyone.

[1]https://www.counterextremism.com/blog/tech-relies-fallacious-arguments-obstruct-regulatory-efforts-germany's-netzdg

Questions for the Record from Senator Alex Padilla
Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law
"Platform Accountability: Gonzalez and Reform"
March 8, 2023

Questions for Mr. Andrew Sullivan

1. How does Section 230 enable online interactivity?

Response: "The Internet" is really just a word for all the tens of thousands of interconnected networks in the world. These networks are each independently operated. Some of them are access networks, such as what we use when we connect to the Internet via our Internet Service Provider (ISP). Some of them provide services, such as a hosting company that provides technical services to people who put up web pages or run email servers or so forth. Still others ensure content is widely dispersed and easily available—so-called content distribution networks (CDNs). Yet others provide access to services they offer, such as the networks operated by companies like Google and Meta. Many networks include multiple parts of all of these functions. All of these differing entities are included in the scope of Section 230's definition of "interactive computer service," and all are thus protected by Section 230.

What Section 230 does is make sure that all those different operators of online services do not become liable if somebody else online says something nasty or unlawful. In that sense, Section 230 is quite literally a necessary condition to having online interactivity at all. Imagine a world in which, every time somebody said something potentially libelous, every one of the possibly hundreds of companies involved in carrying that speech act over the Internet potentially becomes another defendant in a lawsuit. Any one of those intermediaries could decide to block access to that speech rather than risk a lawsuit. Section 230 contains the recognition that, in an online context, the party that is responsible for particular content is *the party that created it*, and nobody else.

In addition to reducing legal risk to online service providers that would arise from hosting or transmitting users' content (discussed more in response to question 2), Section 230 also provides direct protection to online users themselves to forward, "retweet," or "like" content to other users. Thus, under Section 230, if a social media user sees an interesting news article and brings it to the attention of friends and family, that user will not be liable if the article is later held to be defamatory of someone. This type of online person-to-person interactivity happens literally tens of millions (if not hundreds of millions) of times every day, and it is Section 230 that allows users to engage in this online discourse and exchange of ideas without taking on significant legal risks.

2. During the hearing as well as during the Supreme Court oral argument in *Google v. Gonzalez*, some argued that simply because a company may not have immunity from suit for a particular piece of content it chooses to host, does not mean that it can be found liable for that content. In other words, lack of immunity does not automatically mean liability, which should minimize concerns about limiting the scope of Section 230 protection either via statutory interpretation or legislative amendment. **What are your thoughts on this line of argument?**

Response: It is certainly true that a lack of immunity for hosting some content does not automatically imply liability for that content. But that argument misses one of the primary—and absolutely essential—benefits of Section 230: it provides online service providers (and in the case of start-ups, their investors) with confidence that legal risks and legal costs can be controlled and minimized. Without that confidence, the prospect of hosting or transmitting the content created by hundreds of millions of users (and being potentially liable for whatever is in that content) would certainly discourage rational businesses from providing the services in the first place.

The danger to every service online—especially the hundreds of thousands of startups, small and medium sized companies, and non-profits that do not have the same resources as incumbents—lies not merely in avoiding eventual liability. Defending against a lawsuit costs money—sometimes, a lot of money—and if every claim of liability needs to be litigated in order to determine whether a party is liable, some parties will have a choice: either they will spend a lot of money defending themselves against lawsuits, or else they will restrict the ability of others to post content within sites controlled by the party in question. In other words, if I am a social media operator facing liability for posted content, it would be irrational for me not to constrict who may post and what they may say in the social media site I operate. Even if I think that I will eventually be vindicated as not liable, there is a good chance I will not want to (or cannot afford to) defend against every lawsuit anyone might think to bring.

This is especially true of new entrants to the market. It could be true that successful, well-established players would be able to afford the litigation costs. But a recent entrant will not have the financial muscle to withstand a large number of suits. Removing the protections of Section 230 would likely have the perverse effect of entrenching even more than they already are the largest tech companies. Moreover, it would quite likely cause damage to actors on the Internet that have little if anything to do with the actual speech in question (as discussed more fully in response to question 5).

In his article entitled "Why Section 230 Is Better Than the First Amendment,"[1] Professor Eric Goldman details the critical *procedural* benefits of Section 230 that enable online actors to reduce risks of high litigation costs, including allowing early dismissal of claims, greater predictability, reduction of creative drafting of claims, and avoidance of state conflict of laws questions.[2] To attempt to quantify the financial risks that startup companies might face, Engine (a non-profit advocacy organization that supports technology entrepreneurship), researched litigation costs, and concluded in 2021 that *even with Section 230 protections* a startup would likely face $15,000 to 40,000 in legal costs to defend a single lawsuit about online content, and without Section 230 costs would likely exceed $100,000 or much more.[3] When even some of today's largest online platforms are struggling to make a profit, the ability of online startups that host user content to survive without Section 230 is very doubtful.

At the hearing, some articulated the view that it would be healthy to encourage more lawsuits against online entities. Whether or not that is true for the very large and dominant online platforms, that view would be devastating for the broader Internet ecosystem. This is especially true in the United States, which is one of the few countries in the world that does not have a "loser pays" system for litigation. It costs very little to initiate a lawsuit in the U.S., but as detailed above the cost to defend even a frivolous suit can be significant. Section 230 protects hundreds of millions of ordinary Americans, plus tens (or hundreds) of thousands of small businesses, churches, non-profit organizations, and others, and the vast majority of those protected by Section 230 could be grievously harmed if Congress were to open the litigation floodgates aimed at the Internet.

Moreover, apart from legal and financial risks posed to small businesses and others, Congressional action that increases the risk of litigation over online content would certainly lead to the suppression of speech online. In many cases—even frivolous cases—the defendant company would have no practical choice but to agree to remove or block the content targeted in the lawsuit. Even for larger companies, it often is simply not worth the cost of litigation to defend a piece of speech posted by a customer. This would create a powerful 'heckler's veto' that bad actors could exploit: any speech by disfavored minorities, or that is at all controversial in our society, or that any segment of our society might want to suppress, would be at risk of suppression simply because it does not make business sense for a company to pay tens or hundreds of thousands of dollars to fight to keep a particular piece of content online.

---

[1] Goldman, Eric, *Why Section 230 Is Better Than the First Amendment,* Notre Dame Law Review, Vol. 95, No. 33, 2019, available at SSRN: https://ssrn.com/abstract=3351323 or http://dx.doi.org/10.2139/ssrn.3351323.

[2] *Id.* at 39-44.

[3] Engine, *Startups, Content Moderation, and Section 230* (2021), available at https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/61b26e51cdb21375a31d312f/1639083602320/Startups%2C+Content+Moderation%2C+and+Section+230+2021.pdf.

3. As the title of the hearing properly alludes to, there's a lot of Congressional and public interest in ensuring that we have a legal and regulatory environment that enables consumers and regulators to hold companies accountable for their own harmful conduct.

    a. **Under existing Section 230 caselaw such as the 2008 Ninth Circuit decision in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC* and recent Fourth Circuit decision in *Tyrone Henderson, Sr. v. The Source for Public Data, L.P.*, how can platforms be held accountable for their own conduct?**

Response: Section 230 does not protect against liability for *every* action. Instead, it protects intermediaries and users from liability for *content posted by others*.

If an intermediary's own intentional actions create a harm that is independent of any harm that might be caused by content provided by others, to a non-lawyer (like me) that would appear to be outside of the protection of Section 230. Thus, as alleged in *Roommates.com*, if the website questions created by a roommate matching service themselves violate a federal housing statute, then Section 230 would not apply. If, as apparently alleged in the *Henderson* case, the defendant created and published its "own internally created summaries" of criminal charges, then again it would seem that Section 230 would not apply to such summaries (but that case is still in active litigation, differing federal judges disagreed, and we have not looked closely at the underlying court papers, and so we don't have a position on whether that particular decision was correct). Similarly, beyond those two examples, if a company intentionally chooses to display content in a discriminatory manner based on a legally protected class—such as the race of the site visitor—that also would appear to be outside of Section 230.

One important distinction to make is that some "actions" of online intermediaries are—and should be—protected by Section 230 (and I understand also likely protected by the First Amendment). Section 230 expressly protects decisions by an online intermediary to organize, select, and display content submitted by users, and most online sites could not function without protection for the actions of organizing, selecting, and displaying content. That activity is exactly what Congress in the mid-1990s had the foresight to understand would necessarily be done by computer programs rather than humans, and for the Internet to function as a useful information access system, such organization and display of content must be protected.

b. What tools are available to consumers and regulators to hold platforms accountable for their own harmful conduct?

Response: The answer to this question depends on the nature of the harm and the nature of the accountability desired. For instance, Section 230 already does not protect anyone from federal criminal liability when crimes are committed. In the *Gonzalez* case, the United States could have brought charges against the service provider if it concluded that the provider acted unlawfully. It is possible that some of the things Congress wishes to control could be criminal offenses, and Section 230 would offer no protection there.

In addition, some of the issues that get blamed on Section 230 are actually other kinds of failures. For instance, many Americans understandably express concern about tracking and targeting of information or advertising. Yet comprehensive privacy legislation would tackle such issues more directly, by allowing people to avoid or control such tracking in the first place. That in turn would give users much greater control over what information online services can use to target content and advertisements. Similarly, some concerns about the harms from platforms are really rooted in concerns about corporate size and influence—a problem in no way confined to tech platforms.

More broadly, as my initially testimony addressed on pages 5-6, Section 230 is a very poor vehicle for Congress to use to address many of the significant concerns about content on the Internet. Because Section 230 provides essential protection to a huge diversity of service providers—most of which do not have and should not have visibility into the content of communications—carving out new categories of content that would not be covered by Section 230 will impose significant legal risk on parties that have little to no ability to address the harm identified. A new carve out of content from Section 230 would impose legal risk on, for example, the thousands of small Internet Service Providers that provide crucial Internet access in rural, minority, and other underserved areas of the United States. Although the largest ISPs in the country have large legal staffs and significant financial resources, some smaller ISPs would be threatened by even a single lawsuit enabled by reducing Section 230's protections.

4. In her testimony Professor Franks suggests that we consider amending Section 230 to limit the scope of the provision to speech as opposed to "information" by replacing the word "information" in Section 230(c)(1) with "speech." **What are your thoughts on this proposal?**

Response: It is hard to know what impact it would have, for two reasons. First, it seems likely that, at the very least, a vast array of information online is effectively conveyed by something we (and the courts) are likely to recognize as speech. So, on its face, the proposal does not seem likely to satisfy the desire to alter Section 230 in the interests of various social goals. In addition, the Supreme Court and other courts of the United States

have recognized many kinds of actions as effectively being speech anyway—perhaps most notably, spending money.

At bottom, we have not seen a sufficient explanation of the proposed change, and what exactly is included in "information" that is not included in "speech." In Professor Franks' paper in which she first proposed this wording change,[4] she included a list of online "products":

> search engines, social media, online publications with comments sections, Wikis, private message boards, matchmaking apps, job search sites, consumer review tools, digital marketplaces, Airbnb, cloud storage companies, podcast distributors, app stores, GIF clearinghouses, crowdsourced funding platforms, chat tools, email newsletters, online classifieds, video sharing venues …,

and then asserted that "many of these 'products' have very little to do with speech …."[5] But it is wholly unclear which of the listed online services do not involve speech, and in our view the great majority of them precisely involve the type of user-contributed speech that Section 230 was designed to facilitate. And for any online sites that in fact do not involve content posted online by others, such sites would not in any event be protected by Section 230.

---

[4] Franks, Mary Anne, *Reforming Section 230 and Platform Liability*, Cyber Policy Recommendations for the New Administration, STANFORD CYBER POLICY CENTER, Jan. 27, 2021, available at SSRN: https://ssrn.com/abstract=4213840 or http://dx.doi.org/10.2139/ssrn.4213840.

[5] *Id.* at 7-8. In her testimony in this hearing, Professor Franks identified a different list of activities as not being speech: "paying bills, selling stolen goods, shopping for dog leashes, booking hotel rooms, renewing driver's licenses." We could easily agree that paying an electric bill on the electric company website, or renewing a license on a government website, may not involve speech covered under Section 230, but that does not seem to support any change to the language of Section 230. On the other hand, if a maker of craft dog leashes sells them on the Etsy marketplace, the seller very likely describes the dog leashes for sale, and Etsy is likely protected from liability under Section 230 if a dog leash is misdescribed. But it is unclear how changing the statutory language of Section 230 from "information" to "speech" would impact that protection (as courts have clearly held that offering products for sale is a form of speech).

5. Congressional debates about intermediary liability reform are usually rhetorically limited to those actors that operate at application layer of the Internet. However, as you shared in your testimony, Section 230 extends to the infrastructure intermediaries below them. You highlighted in particular: Internet Service Providers, Content Delivery Networks and Web Hosting Companies.

   a. What should legislators know about the different kinds of intermediaries protected by Section 230?

Response: The rich set of networks, services, and information on the Internet is made possible by a vast set of supporting services and infrastructure, much of which operate smoothly out of the view or interest of the public or policymakers. Every single one of these elements of our online environment depend on the protections of Section 230 in their normal everyday operation. As discussed above, Section 230 amendments aimed at the application layer (which is where the major online platforms generally operate) run the risk of creating collateral damage—regulatory shrapnel, if you will—that can do grave and unknown damage to the machinery of the Internet.

On the other hand, it would not be straightforward to craft a Section 230 amendment narrowly tailored to the "application layer" of the Internet. While the idea of the application layer can in general terms be simply explained, actually deciding what is an application and what is in that layer is extraordinarily difficult. This is related to the difficulty of understanding each of the intermediaries mentioned in the question.

For instance, when you visit a web page, the web page *looks* like a single thing. This is part of the technical ingenuity of the Internet, because in fact a web page can be assembled out of many different parts, which may be provided by many different providers. To give an example, in a web page with video embedded, very often the video content is widely distributed through the use of a Content Delivery (sometimes "Distribution") Network (CDN). This is done so that everyone does not have to fetch a very large file from a single source on the Internet, because that would be slow and unsatisfying to the viewer and would increase network congestion. CDNs work well when they are completely agnostic about the content of the files they are distributing. To a CDN, every file is just a "bag of bits" to be distributed as quickly and efficiently around the Internet as possible. CDNs can act this way because they are not liable for those contents. If they became liable, they would have to examine every file and make their own determinations of their liability. This would not only slow service. It also represents the potential for corporate censorship as well as privacy violations.

In addition, the example above is for a web page that has only a single video embedded. But many web pages are much more complicated than that, with multiple different items embedded within the single web page. Each of these might be coming from a different source—perhaps the website operator, perhaps a different website, perhaps a CDN (not

necessarily the same CDN as the video), and so forth. All of this happens in milliseconds, so that your visit to the web page works exactly as you expect it to. But every one of those sources that make up the web page you are visiting are protected by Section 230.

Similarly, Internet Service Providers (ISPs) and Web Hosting Companies also rely on the same intermediary liability protections. It would be impossible for a large web host, for instance, to know all the content posted on machines they are operating. Imposing such liability would dramatically disrupt and threaten the current functioning of the Internet.

Moreover, it is not only liability protection from content posted by others that intermediaries get in Section 230. They *also* get protection from liability for their good faith efforts to manage problems that they see on their platforms. For instance, many concerns about Section 230 protections focus on the items that platforms do not remove from their systems. But equally vexing are cases where platforms remove content that may turn out not to be a problem, but that they believe to be dangerous due to automated content monitoring and so forth. Protecting such well-meaning activities from liability is *also* important, because it enables the very kinds of content moderation that some in society think platforms should do more aggressively.

b. How should these differences inform proposals to amend Section 230?

Response: The reality is that actually amending Section 230 would be devilishly hard to do. Because the Internet is made of so many different pieces, even describing all the relevant parties in legislation is difficult—and that is before we recognize that some kinds of entities and services might not have been invented yet. This is exactly what is at stake: the Internet was designed to be built upon, and is constantly evolving and changing. It is a tool of creativity and innovation, and Section 230—which used broad statutory categories to allow evolution—is essential to enabling that innovation.

That is, part of what has made the Internet so important is that it is itself an environment of innovation. Even the large platforms present a home for such innovation, where people find ways to address social ills. Plenty of addicts have found their way to recovery through Google searches or Facebook friends. Many at-risk youths in communities facing disproportionate rates of suicide are alive today because they found help and made connections with peers through outreach campaigns like We Matter on platforms like Facebook and YouTube. News that is important to a widely-dispersed community of people, and that would never have been reported in traditional media, becomes an opportunity to create community online. Political viewpoints—whether left, right, or center—that were once too small to form communities at all can now debate and work out political programs as part of the great American tradition of public debate. Medical miracles that once had to spread at the speed of journal articles and postal mail can now happen because scientists collaborate, sometimes even in real time, with their earliest

scientific results. Experts in medicine, agriculture and other disciplines can advise remote communities over the Internet. People cheerfully give away—in videos, in web pages, and in online discussion forums—the expert fruits of their labor, just to help one another.

None of these things were, exactly, predicted in advance. The founders of the Internet understood that they were producing a tool for human collaboration, and people who make tools inevitably make tools to make other tools. We are the inheritors of that beautiful, human tradition. Some of the very best of humanity is available online, every day, and we should not forget that.

Now, I do not pretend that the Internet—or platforms that operate within it—enable only humanitarian efforts. In that way, the Internet is no different from previous communication technologies. Written letters could be used to promote sedition. The printing press spread falsehoods as well as truth. Telegraph, radio, and television have all been used to hurt as well as help. What the Internet brings is its interactive nature: the ability of anyone to talk to anyone or even everyone, and the ability of everybody else to respond. That brings, unquestionably, dangers, but it also brings the sort of debate, uncontrolled by any gatekeeper, that the Founders of the United States of America valued and promoted. Intermediaries on the network of all kinds are implicated in ensuring that kind of conversation can happen. Hasty or broad changes to Section 230, therefore, could be extremely bad for American society.

As noted above in response to question 1, Section 230 seeks to ensure that the person most directly responsible for a violation of law or other harm is the one who should be held accountable for it. Most often that will be the creator or poster of the offending content. Sometimes, an online platform might directly violate a law (as suggested in the Roommates.com scenario mentioned in question 3a). But very seldom will the appropriate party to be held liable be an Internet Service Provider, or a CDN, or a web hosting company, or any of the many other intermediaries that are essential to making the Internet function. And because Section 230 protects the full range of Internet users and intermediaries—and not just online platforms—it is a very poor vehicle which with to address social problems at the "application layer."

As Congress continues its focus on addressing significant social concerns in the online environment, it will be important to apply some analytic framework to any proposed regulation of the Internet. Any such framework must allow an understanding of what the proposal might do—not just in the cases where it is aimed, but also in the cases where it is not. The Internet Society has an Internet Impact Assessment Toolkit[6] that is intended to assist with those kinds of explorations, and we stand ready to help the Congress make those kinds of evaluations.

---

[6] https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/.

February 10, 2023

To the Honorable Chair Durbin, Ranking Member Graham, and Members of the Senate Judiciary Committee.

Dear Chairman Durbin,

My name is Anastasia, I'm 18 years old, and my childhood was stolen from me when explicit videos of me being sexually abused were distributed on the internet. The trauma of having my abuse forever immortalized on the internet is something I will never be able to escape. To this day they likely are still on thousands of peoples phones. My abuser continues to roam free and traumatize other young girls.

Companies create a hyper complex process to take down content which ends up being impossible for the average adult let alone a child to navigate. Omegle, which is an app designed to connect strangers to strangers via video chat, offered an anonymous platform for my abuser to recruit other young victims. It also offered him a platform to anonymously molest children on live video. He would use tags like "One Direction" or "Hannah Montana" to directly target a young audience.

Despite countless reports to NCMEC, Reddit, Omegle, and Twitter, my abuse material continues to live and spread on the Internet. But my story is not unique. In 2022 alone, 322 million files of child sexual abuse material were found online. That number is equivalent to the entire population of the United States, but it's believed to represent only 3% of all child sexual abuse material available on the Internet.

As more and more children start using online platforms at younger ages, this number will only continue to rise. In LA County alone, we have found over 100 cases in the last year against Omegle and Kik regarding child exploitation. This issue will continue to exacerbate, as evidenced by the fact that the number of victims of online grooming tripled during the COVID-19 pandemic.

My name is Saanvi. I'm also 18 years old. Cultural differences in my family denied me the opportunity to have conversations about sexual violence at home, education which I know is disproportionately withheld from children of color. Because of this, me and so many kids like me have no idea what's going on when they unknowingly interact with predators online.

Upon getting to know each other and sharing our experiences, Ani and I decided to research the current legal grounds that allow minors to hold platforms like Omegle accountable for the abuse that they permit. It was devastating for us to learn that despite the overwhelming amount of evidence that corroborates the urgency to address this issue, there is little to no legal basis for victims of child sexual abuse to seek legal action against the platforms that permit their violence to occur. Dozens of court cases at the state level have been dismissed on these claims. Thousands of our peers have already been denied any means to hold their abuser or the platform that facilitated their abuse accountable, and millions will continue to be denied access to justice due to the dangerous precedent that current law forces our courts to set.

Every day, abusers take advantage of the features that online platforms such as Omegle, Kik, and Reddit provide under the guise of "safety;" almost all of them allow users to retain some modicum of anonymity,

making predators difficult to spot and even more difficult to track. This leaves thousands of cases unreported, as predators are given a digital curtain to hide behind. Additionally, scraping algorithms allow child sexual abuse material posted on or through these platforms to automatically get reposted to dozens of more covert websites where there is no mechanism to report content or even contact service providers to manage the material posted. This means that even if the material is removed from these larger, more mainstream platforms, the material still lives and spreads throughout the internet through more hidden channels.

This, coupled with the fact that platforms are immune to liability for facilitating child sexual abuse or distributing CSAM means that while the law explicitly prohibits the sexual abuse of or distribution of content pertaining to minors, such violence still occurs without culpable parties facing any consequences. Rather, the burden of dealing with this issue is placed on victims, who are told to "move on" without any recourse for their trauma because there are limited legal grounds for them to pursue this kind of action.

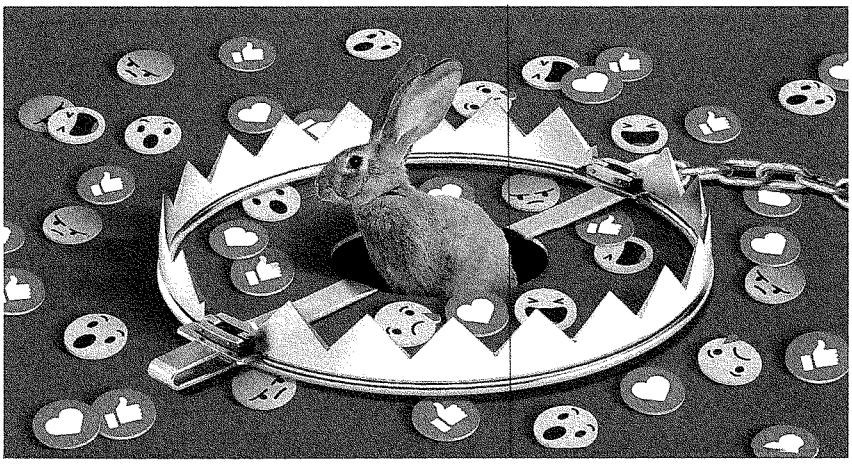
Every explicit photo of a child is a photo of a tortured child. As predators have continued to adapt to the internet, our safety measures have lagged behind. Thus, we urge you to take the necessary steps to end the injustices that 29 million survivors across the United States currently face by regulating the means through which Internet-based service providers currently profit off of child abuse.

Best,
Saanvi Arora and Ani Chaglasian

TECH NEWS

'Carol's Journey': What Facebook knew about how it radicalized users

Internal documents suggest Facebook has long known its algorithms and recommendation systems push some users to extremes.



— Internal Facebook documents detail how researchers employed by the company found that the platform radicalized some users and created fringe groups with outsize impact. Doug Chayka for NBC News

SAVE

Oct. 22, 2021, 3:31 PM PDT / Updated Oct. 26, 2021, 9:50 AM PDT

By Brandy Zadrozny

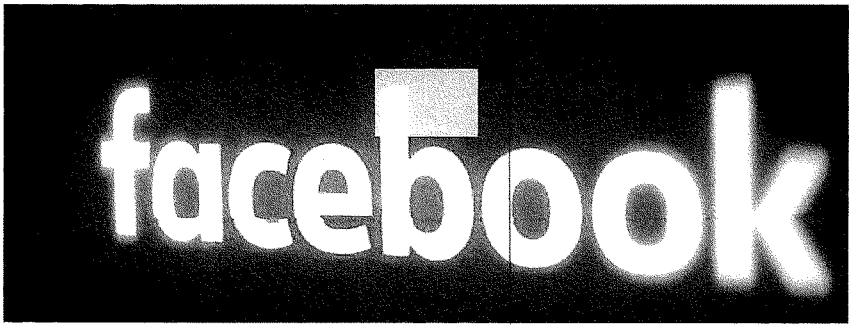
In summer 2019, a new Facebook user named Carol Smith signed up for the platform, describing herself as a politically conservative mother from Wilmington, North Carolina. Smith's account

indicated an interest in politics, parenting and Christianity and followed a few of her favorite brands, including Fox News and then-President Donald Trump.

Though Smith had never expressed interest in conspiracy theories, in just two days Facebook was recommending she join groups dedicated to QAnon, a sprawling and baseless conspiracy theory and movement that claimed Trump was secretly saving the world from a cabal of pedophiles and Satanists.

Smith didn't follow the recommended QAnon groups, but whatever algorithm Facebook was using to determine how she should engage with the platform pushed ahead just the same. Within one week, Smith's feed was full of groups and pages that had violated Facebook's own rules, including those against hate speech and disinformation.

Internal documents reveal Facebook knew of platform's harms



Smith wasn't a real person. A researcher employed by Facebook invented the account, along with those of other fictitious "test users" in 2019 and 2020, as part of an experiment in studying the platform's role in misinforming and polarizing users through its recommendations systems.

That researcher said Smith's Facebook experience was "a barrage of extreme, conspiratorial, and graphic content."

The body of research consistently found Facebook pushed some users into "rabbit holes," increasingly narrow echo chambers where violent conspiracy theories thrived. People radicalized through these rabbit holes make up a small slice of total users, but at Facebook's scale, that can mean millions of individuals.

The findings, communicated in a report titled "Carol's Journey to QAnon," were among thousands of pages of documents included in disclosures made to the Securities and Exchange Commission and provided to Congress in redacted form by legal counsel for Frances Haugen, who worked as a Facebook product manager until May. Haugen is now asserting whistleblower status and has filed several specific complaints that Facebook puts profit over public safety. Earlier this month, she testified about her claims before a Senate subcommittee.

Versions of the disclosures – which redacted the names of researchers, including the author of "Carol's Journey to QAnon" – were shared digitally and reviewed by a consortium of news organizations, including NBC News. The Wall Street Journal published a series of reports based on many of the documents last month.

"While this was a study of one hypothetical user, it is a perfect example of research the company does to improve our systems and helped inform our decision to remove QAnon from the platform," a Facebook spokesperson said in a response to emailed questions.

Facebook CEO Mark Zuckerberg has broadly denied Haugen's claims, defending his company's "industry-leading research program" and its commitment to "identify important issues and work on them." The documents released by Haugen partly support those claims, but they also highlight the frustrations of some of the employees engaged in that research.

Facebook whistleblower: Company puts 'profits before people'

Among Haugen's disclosures are research, reports and internal posts that suggest Facebook has long known its algorithms and recommendation systems push some users to extremes. And while some managers and executives ignored the internal warnings, anti-vaccine groups, conspiracy theory movements and disinformation agents took advantage of their permissiveness, threatening public health, personal safety and democracy at large.

"These documents effectively confirm what outside researchers were saying for years prior, which was often dismissed by Facebook," said Renée DiResta, technical research manager at the Stanford Internet Observatory and one of the earliest harbingers of the risks of Facebook's recommendation algorithms.

Facebook's own research shows how easily a relatively small group of users has been able to hijack the platform, and for DiResta, it settles any remaining question about Facebook's role in the growth of conspiracy networks.

"Facebook literally helped facilitate a cult," she said.

'A pattern at Facebook'

For years, company researchers had been running experiments like Carol Smith's to gauge the platform's hand in radicalizing users, according to the documents seen by NBC News.

This internal work repeatedly found that recommendation tools pushed users into extremist groups, findings that helped inform policy changes and tweaks to recommendations and news feed rankings. Those rankings are a tentacled, ever-evolving system widely known as "the algorithm" that pushes content to users. But the research at that time stopped well short of inspiring any movement to change the groups and pages themselves.

That reluctance was indicative of "a pattern at Facebook," Haugen told reporters this month. "They want the shortest path between their current policies and any action."

"There is great hesitancy to proactively solve problems," Haugen added.

A Facebook spokesperson disputed that the research had not pushed the company to act and pointed to changes to groups announced in March.

While QAnon followers committed real-world violence in 2019 and 2020, groups and pages related to the conspiracy theory skyrocketed, according to internal documents. The documents also show how teams inside Facebook took concrete steps to understand and address those issues – some of which employees saw as too little, too late.

By summer 2020, Facebook was hosting thousands of private QAnon groups and pages, with millions of members and followers, according to an unreleased internal investigation.

A year after the FBI designated QAnon as a potential domestic terrorist threat in the wake of standoffs, alleged planned kidnappings, harassment campaigns and shootings, Facebook labeled QAnon a "Violence Inciting Conspiracy Network" and banned it from the platform, along with militias and other violent social movements. A small team working across several of Facebook's departments found its platforms had hosted hundreds of ads on Facebook and Instagram worth thousands of dollars and millions of views, "praising, supporting, or representing" the conspiracy theory.

The Facebook spokesperson said in an email that the company has "taken a more aggressive approach in how we reduce content that is likely to violate our policies, in addition to not recommending Groups, Pages or people that regularly post content that is likely to violate our policies."

For many employees inside Facebook, the enforcement came too late, according to posts left on Workplace, the company's internal message board.

"We've known for over a year now that our recommendation systems can very quickly lead users down the path to conspiracy theories and groups," one integrity researcher, whose name had been redacted, wrote in a post announcing she was leaving the company. "This fringe group has grown to national prominence, with QAnon congressional candidates and QAnon hashtags and groups trending in the mainstream. We were willing to act only * after * things had spiraled into a dire state."

'We should be concerned'

While Facebook's ban initially appeared effective, a problem remained: The removal of groups and pages didn't wipe out QAnon's most extreme followers, who continued to organize on the platform.

"There was enough evidence to raise red flags in the expert community that Facebook and other platforms failed to address QAnon's violent extremist dimension," said Marc-André Argentino, a research fellow at King's College London's International Centre for the Study of Radicalisation, who has extensively studied QAnon.

Believers simply rebranded as anti-child-trafficking groups or migrated to other communities, including those around the anti-vaccine movement.

It was a natural fit. Researchers inside Facebook studying the platform's niche communities found violent conspiratorial beliefs to be connected to Covid-19 vaccine hesitancy. In one study, researchers found QAnon community members were also highly concentrated in anti-vaccine communities. Anti-vaccine influencers had similarly embraced the opportunity of the pandemic and used Facebook's features like groups and livestreaming to grow their movements.

"We do not know if QAnon created the preconditions for vaccine hesitancy beliefs," researchers wrote. "It may not matter either way. We should be concerned about people affected by both problems."

SOCIAL MEDIA

Big tech was a target at CPAC, but conservative startups face challenges

QAnon believers also jumped to groups promoting former President Donald Trump's false claim that the 2020 election was stolen, groups that trafficked in a hodgepodge of baseless conspiracy theories alleging voters, Democrats and election officials were somehow cheating Trump out of second term. This new coalition, largely organized on Facebook, ultimately stormed the U.S. Capitol on Jan. 6, according to a report included in the document trove and first reported by BuzzFeed News in April.

These conspiracy groups had become the fastest-growing groups on Facebook, according to the report, but Facebook wasn't able to control their "meteoric growth," the researchers wrote, "because we were looking at each entity individually, rather than as a cohesive movement." A Facebook spokesperson told BuzzFeed News it took many steps to limit election misinformation but that it was unable to catch everything.

Facebook's enforcement was "piecemeal," the team of researchers wrote, noting, "we're building tools and protocols and having policy discussions to help us do this better next time."

'A head-heavy problem'

The attack on the Capitol invited harsh self-reflection from employees.

One team invoked the lessons learned during QAnon's moment to warn about permissiveness with anti-vaccine groups and content, which researchers found comprised up to half of all vaccine content impressions on the platform.

"In rapidly-developing situations, we've often taken minimal action initially due to a combination of policy and product limitations making it extremely challenging to design, get approval for, and roll out new interventions quickly," the report said. QAnon was offered as an example of a time when Facebook was "prompted by societal outcry at the resulting harms to implement entity takedowns" for a crisis on which "we initially took limited or no action."

The effort to overturn the election also invigorated efforts to clean up the platform in a more proactive way.

Facebook's "Dangerous Content" team formed a working group in early 2021 to figure out ways to deal with the kind of users who had been a challenge for Facebook: communities including QAnon, Covid-denialists and the misogynist incel movement that weren't obvious hate or terrorism groups but that, by their nature, posed a risk to the safety of individuals and societies.

The focus wasn't to eradicate them, but to curb the growth of these newly branded "harmful topic communities," with the same algorithmic tools that had allowed them to grow out of control.

"We know how to detect and remove harmful content, adversarial actors, and malicious coordinated networks, but we have yet to understand the added harms associated with the formation of harmful communities, as well as how to deal with them," the team wrote in a 2021 report.

In a February report, they got creative. An integrity team detailed an internal system meant to measure and protect users against societal harms including radicalization, polarization and discrimination that its own recommendation systems had helped cause. Building on a previous research effort dubbed "Project Rabbithole," the new program was dubbed "Drebbel." Cornelis Drebbel was a 17th-century Dutch engineer known for inventing the first navigable submarine and the first thermostat.

The Drebbel group was tasked with discovering and ultimately stopping the paths that moved users toward harmful content on Facebook and Instagram, including in anti-vaccine and QAnon groups.

A post from the Drebbel team praised the earlier research on test users. "We believe Drebbel will be able to scale this up significantly," they wrote.

"Group joins can be an important signal and pathway for people going towards harmful and disruptive communities," the group stated in a post to Workplace, Facebook's internal message board. "Disrupting this path can prevent further harm."

The Drebbel group features prominently in Facebook's "Deamplification Roadmap," a multistep plan published on the company Workplace on Jan. 6 that includes a complete audit of recommendation algorithms.

In March, the Drebbel group posted about its progress via a study and suggested a way forward. If researchers could systematically identify the "gateway groups," those that fed into anti-vaccination and QAnon communities, they wrote, maybe Facebook could put up roadblocks to keep people from falling through the rabbit hole.

The Drebbel "Gateway Groups" study looked back at a collection of QAnon and anti-vaccine groups that had been removed for violating policies around misinformation and violence and incitement. It used the membership of these purged groups to study how users had been pulled in. Drebbel identified 5,931 QAnon groups with 2.2 million total members, half of which joined through so-called gateway groups. For 913 anti-vaccination groups with 1.7 million members, the study identified 1 million had joined via gateway groups. (Facebook has said it recognizes the need to do more.)

Facebook integrity employees warned in an earlier report that anti-vaccine groups could become more extreme.

"Expect to see a bridge between online and offline world," the report said. "We might see motivated users create sub-communities with other highly motivated users to plan action to stop vaccination."

A separate cross-department group reported this year that vaccine hesitancy in the U.S. "closely resembled" QAnon and Stop the Steal movements, "primarily driven by authentic actors and community building."

"We found, like many problems at FB," the team wrote, "that this is a head-heavy problem with a relatively few number of actors creating a large percentage of the content and growth."

The Facebook spokesperson said the company had "focused on outcomes" in relation to Covid-19 and that it had seen vaccine hesitancy decline by 50 percent, according to a survey it conducted with Carnegie Mellon University and the University of Maryland.

Whether Facebook's newest integrity initiatives will be able to stop the next dangerous conspiracy theory movement or the violent organization of existing movements remains to be seen. But their policy recommendations may carry more weight now that the violence on Jan. 6 laid bare the outsize influence and dangers of even the smallest extremist communities and the misinformation that fuels them.

"The power of community, when based on harmful topics or ideologies, potentially poses a greater threat to our users than any single piece of content, adversarial actor, or malicious network," a 2021 report concluded.

The Facebook spokesperson said the recommendations in the "Deamplification Roadmap" are on track: "This is important work and we have a long track record of using our research to inform changes to our apps," the spokesperson wrote. "Drebbel is consistent with this approach, and its research helped inform our decision this year to permanently stop recommending civic, political or news Groups on our platforms. We are proud of this work and we expect it to continue to inform product and policy decisions going forward."

CORRECTION (Oct. 22, 2021, 7:06 p.m. ET): A previous version of this article misstated the purpose of a study conducted by Facebook's Drebbel team. It studied groups that Facebook had removed, not those that were currently active.

CORRECTION (Oct. 23, 2021, 9:44 a.m. ET): A previous version of this article misstated a finding of Facebook research into anti-vaccination groups. It found one million people had joined anti-vaccination groups through gateway groups, not that there were one million gateway groups.

Brandy Zadrozny

Brandy Zadrozny is a senior reporter for NBC News. She covers misinformation, extremism and the internet.

European Commission

Home > Research and Innovation > Projects > Success stories > All success stories > Deconstructing the terrorism discourse on social media

Deconstructing the terrorism discourse on social media

Although social media has infiltrated our daily lives and become a powerful tool it is not always put to good use. EU-funded research is looking at how the Islamic State group has used social media to promote the terrorist agenda and attract followers – and aims to shape policy to counter this movement.

© moi3r #134050212, 2019 source: stock.adobe.com

17 APR 2019

Social media use has increased dramatically over the past decade and is now a major source of information and influence. Used legitimately, it is a vital tool for communication. Unfortunately, it can help groups and individuals with less positive intentions to promote violent ideologies, create confusion and spread fear among the general public.

The EU-funded MWDIR project has spent two years investigating how the ideology of Islamic radicalism is being legitimised and spread through social media content. In particular, lead researcher Mohammedwasem Amer has focused on the terrorist organisation Islamic State (IS) to determine why its ideas are so persuasive for certain demographics in Western countries and how this leads to the radicalisation of young people in the EU and worldwide.

Amer argues that the development and accessibility of social media has helped IS and other terrorist, extremist and radical movements expand their reach to a wide range of audiences around the world.

'We set out to examine IS' social media strategies, practices and presence on the internet,' he explains. 'Our analysis should help raise awareness of how social media is being used for the radicalisation of certain populations and the legitimation of the terrorist discourse. Through a better understanding of the strategies used, both technologically and in terms of rhetorical devices, we can also better inform policy to counter this phenomenon.'

Amer adds that 'the more we analyse and understand terrorist organisations' presence and ideological discourses on social media, the more effective ways we can find to counter the kind of terrorist propaganda that may lead to violent actions against innocent people in Europe and all over the world.'

The research is funded by the EU's Marie Skłodowska-Curie fellowship programme.

+ Add to pdf basket

PDF Basket

No article selected

Project details

Project acronym
MWDIR
Project number
707482
Project coordinator
United Kingdom
Project participants:
United Kingdom
Total cost
€ 195 454
EU Contribution
€ 195 454
Project duration
February 2017 - January 2019

See also

https://cordis.europa.eu/project/rcn/204939/factsheet/en

Related R&I themes

Marie Skłodowska-Curie Actions
Information society
Information technology
Internet
Telecommunications
Innovation
Security

All success stories

Country
- Any -
Theme
- Any -
Framework programme
- Any -
Project acronym
- Any -
Project coordinator
Project start date
YYYY-MM-DD
Project end date
YYYY-MM-DD
Find

This story in other languages

Share this page

Twitter | Facebook | LinkedIn | E-mail | More share options

European Commission website

This site is managed by the Directorate-General for Research and Innovation

Strategy
About the European Commission
Business, Economy, Euro
Live, work, travel in the EU
Law
Funding, Tenders
Research and innovation
Energy, Climate change, Environment
Education

Aid, Development cooperation, Fundamental rights
Food, Farming, Fisheries
EU regional and urban development
Jobs at the European Commission
Statistics
News
Publications

Contact the European Commission
Language policy

Your cookie preferences have been saved. To change your preferences at any time, see our cookies policy or visit the link in the page footer. Close

Eric Schnapper

From: Nitsana Darshan-Leitner <nitsanaleitner@gmail.com>
Sent: Sunday, March 05, 2023 10:17 AM
To: Eric Schnapper; Jill Gelhausen; Keith Altman; Leitner; Robert Tolchin
Subject: Hearing

Hi Eric,

We have a problem with your overly lawyerly written opening. We understand your point about being "contrived" but there is no guarantee that you'll have the opportunity later during questioning to raise the points of concern to our clients and us. Who knows what they'll ask you and then the opportunity will be lost. It's too risky to assume you can sneak it in later. The panel is entitled *Gonzalez, Reform and Accountability*, and we need to focus at least in part on the issues of benefit and real concern to the Gonzalezes and other terror victims - namely receiving Justice and compensation for the devastation their families had inflicted upon them. We can't allow it just be about some theoretical free speech issues argued by law professors at an academic conference.

We have been trying to get a Congressional hearing on Section 230 for years and only now the Senate, in the wake of Gonzalez, arose from their slumber. We can't miss this opportunity, we might not receive another one

We did not bring these suits to help Yelp, Reddit, Airbnb and Tik Tok find a way to navigate the federal code so they can continue to make billions. We brought them to stop terror on the web and get compensation ($$$$) from the platforms for the families who put their trust in us. Approaching it like this is a constitutional law course exam with theoretical 1st Amendment fact patterns does nothing to help the Gonzalezes, the Taamnehs, the Forces or the others with murdered children. It cannot just be about whether Trump and Musk can be allowed to tweet their right wing stupidity as Hawley no doubt is focused on.

The Senate is only finally acting now with a snap hearing because of all the criticism they have been facing in the media (after the Supreme Court arguments) about them being too divided & lame to take up the issue and do their elected jobs on their own. The hearing is called "Platform Accountability." I understand your goal is to be reasonable and workmanlike so you can continue to provide input to the Committee and have future involvement. But completely ignoring the current elephant in the room robs the clients of any benefit from the Senate being embarrassed into action. The terror victims of the past need to be mentioned. It has to be retroactive as well. What was dryly argued before the Court at the hearing was not so well received. The justices dismissed it as technological mumbo jumbo beyond their competence. You need to humanize it a little, as this is what is at stake - not merely whether Facebook shareholders will get a bigger dividend this quarter.

As such, we really urge you to include these points even briefly in at least one paragraph of your written statement to the Committee:

1. The social media is overrun with hate speech, incitement to terrorism and calls for antisemitic violence. That the social media platforms have repeatedly refused to take any action to self regulate fearing it will endanger their profitability & business models. That Section 230, as it's wrongly been applied by the lower courts provides them an undeserved blanket immunity that resulted in the murder and maiming of your client, Nohemi Gonzalez, a Mexican-American student and other innocent victims worldwide.

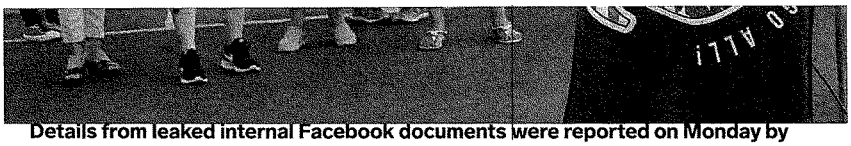
2. That the Congress never intended 230 to be carte blanche immunity and they need to act to curtail the criminal messaging and aiding and abetting of terrorism (and defend the safety of US citizens) being routed through the social media servers located in Palo Alto, California.

I am told all 5 witnesses will sit as a panel. Each will get about 5minutes for opening remarks, and the rest of the hearing will be questions from the subcommittee.

--
--
Nitsana Darshan-Leitner, Esq.10 Hata'as St., Ramat Gan 52512 Israel Tel: 972-3-7514175 Fax: 972-3-7514174 nitsanaleitner@gmail.com

Facebook recommended QAnon groups to a new user within 2 days of joining the platform, according to a new whistleblower report

Kieran Press-Reynolds Oct 25, 2021, 1:45 PM



Details from leaked internal Facebook documents were reported on Monday by several news outlets.

One document, "Carol's Journey to QAnon," reportedly shows how a new user found QAnon content.

A researcher reportedly said the user faced "a barrage of extreme, conspiratorial" content.

Facebook recommended QAnon groups to a new user within two days of them joining ording to leaked internal research documents reportedly obtained by

Jump to

Main content
Search
Account

rcher created the account for that fictional user, positioned as a

HOMEPAGE

Subscribe

NBC News, which said they reviewed the leaked document.

The leaked document showed that Carol Smith had an affinity for politics and parenting, liked pages for former President Donald Trump and Fox News, and had shown zero interest in conspiracy theories before getting pushed toward QAnon content during the experiment in the summer of 2019, NBC News reported. The research, entitled "Carol's Journey to QAnon," was used to track how Facebook's recommendation algorithm could polarize and misinform users, according to NBC News.

QAnon is a web of baseless conspiracy theories that began with the false claim that Trump was fighting against a cabal of "deep state" human traffickers. Believers of QAnon have been accused of several crimes, involving murder and kidnapping, as Insider has reported.

Jump to

Main content
Search
Account

part of the so-called Facebook Papers, an array of thousands of pages
ients reportedly obtained by the whistleblower Frances Haugen, a
anager in Facebook's civic integrity division. Haugen initially

HOMEPAGE

September. An organized group of 17 United States news organizations said they reviewed the papers and published a slew of reports on the leaked internal documents on Monday morning.

Insider did not obtain the documents.

Though Carol Smith did not join any of the QAnon groups she was initially recommended, the algorithm "pushed ahead" with its recommendations, NBC News reported. Within a week, the user's feed was packed with pages and groups that violated Facebook's own hate speech and disinformation guidelines, the leaked research showed, as reported by NBC News.

Carol Smith's Facebook feed became "a barrage of extreme, conspiratorial, and graphic content," the researcher reportedly wrote in the leaked document.

Jump to

Main content
Search
Account

sperson told NBC News in a statement that this research "helped

HOMEPAGE

Subscribe

"significant risks to public safety," including targeting QAnon groups, pages, and accounts that promoted violence. In October 2020, as other social media companies including YouTube and Twitter took stronger stances on QAnon, the company expanded its policy to ban all non-violent QAnon accounts across all its platforms.

When Haugen revealed her identity as the Facebook whistleblower in a "60 Minutes"

During Haugen's testimony before a United States Senate Commerce subcommittee on October 5, she accused the platform of destabilizing democracy, making women and young girls feel bad about their bodies, and prioritizing profit over everything else. She also said that no one holds CEO Mark Zuckerberg "accountable but himself" and suggested that the federal government create an official body to oversee and regulate platforms like Facebook, as Insider reported.

Facebook CEO Mark Zuckerberg responded to Haugen's claims about the platform in a 1,300-word statement on his Facebook page later that day, saying "many of the claims don't make any sense" and denying that the company "prioritize[s] profit over safety and well-being."

National Defence / Défense nationale

Canadian Forces College / Collège des Forces Canadiennes

HOW ISIS USES SOCIAL MEDIA FOR RECRUITMENT

Major Ata AlSarayreh

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019-2020

SOLO FLIGHT

HOW ISIS USES SOCIAL MEDIA FOR RECRUITMENT

By Maj Ata. AlSarayreh

Word Count: 4,953

Nombre de mots : 4.953

HOW ISIS USES SOCIAL MEDIA FOR RECRUITMENT

INTRODUCTION

The combination of affordability, strategic reach, and ability to micro-target your audience by demographics, has made social media platforms the medium of choice for extremist organization, Islamic State of Iraq and Syria (ISIS). At their fingertips, they have access to strategic communication and global recruitment. They merely have to extend their hands and touch their screens. They use Facebook, YouTube, and Twitter with all the ease of those born to it, and are not struggling like traditional militaries full of digital immigrants. In most cases, if not all, terrorists and extremist groups have primarily used this avenue to fuel, intensify, and make their fight international. In today's world, terrorist organizations not only use social media to spread propaganda and recruit, but also to carry out the actual attacks by using their followers to do that in their name. Antonia Ward from the U.S. think tank *RAND* stated in a comprehensive security study that: "ISIS's strategic use of social media demonstrates the resourcefulness of the terrorist-cum-insurgent organization, which mobilized an estimated 40,000 foreign nationals from 110 countries to join the group."[1]

Increasing access to the internet, coupled with its open standards structure is posing significant challenges to international governance, and increasing social strife for domestic security, particularly in vulnerable countries. This medium gives the ISIS militia the opportunity to target a vastly increased recruiting pool, concurrently identifying the extremists, while avoiding detection by respective domestic security authorities. The evidence shows an increased number of people who have been attracted

[1] Antonia Ward, "ISIS's Social Media Use Poses a Threat to Stability in the Middle East and Africa," RAND Corporation Provides Objective Research Services and Public Policy Analysis | RAND, Last modified December 11, 2018, https://www.rand.org/blog/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html.

both from the Middle East and Africa to join the team.[2] Consequently, strategic recruitment has made it possible for ISIS to regain some of its lost territories, and protract the conflict.[3] The importance of social medial as a recruiting instrument for ISIS is inseparable from sustaining their tactical successes. The reach that social media grants, coupled with ISIS's strong narrative, which focuses primarily on religious, social, and material grounds, has made their organization successful and a harbinger of future conflicts.

RESEARCH QUESTIONS

The questions that will be used in this essay, how effective is ISIS' use of various social media platforms? In particular, what themes does ISIS use through social media to attract followers?

This paper will argue that social media was ISIS' most effective strategic tool to increase their ranks and spread their propaganda. It was also a highly effective tactical level tool, used prior to attacks to coerce their enemies and encourage them to flee. However, it was the use of social media within the cognitive domain that provided them with a competitive advantage against both their adversaries and close ideological competitors. Their level of informational dominance and volume of messaging is unexplainable by any other means. Exploring this 'thread' will consist of two defined steps. First will be the analysis of the various platforms that ISIS utilizes to shape, recruit, and brainwash recruits. Second, the argument will shift to a detailed evaluation of the common themes that ISIS utilizes to recruit its targeted individual include branding, recruiting the youths, and its version of love versus hate, in order to illustrate how social

[2] *Ibid.*,1.
[3] *Ibid.*,2.

media, coupled with the right message was able to create a digital community, providing the manpower and financial support that underwrote ISIS' tactical successes.

PLATFORMS

Social Media Theories

ISIS main focus of social media is international recruitment not proselytizing, though these shouldn't be considered completely divisible within the ISIS information campaign framework. It must ensure that it maintains, and increases, a high number of followers to replace those lost as a result of death and desertion. In this context, ISIS has been using different tools to carry out its recruitment process, in which social media use must be considered the most prevalent and ties together more recognizable methods. ISIS' broad approach of recruiting followers enabled by social media, however, is more dangerous and has helped to attain their recruitment targets and objectives.[4] ISIS has developed a brutal but effective approach to inspiring susceptible groups and attracting people to join or finance their cause. This translates into sustaining their militia activities in the field, and their population intimidation campaign, exemplified by their infamous murder cycles. The war in Syria and Iraq has established new social media networks, allowing ISIS to consolidate targeted virtual groups from various Twitter accounts, creating an exploitable and operationalized echo chamber. In doing so, ISIS can obtain not only the names of potential recruits but was also capable of mapping potential ISIS supporter profiles to further refine their messaging, increasing their social engineering efficacy.[5]

---

[4] Sarah Ponder and Jonathan Matusit, "Examining ISIS Online Recruitment through Relational Development Theory," Connections: The Quarterly Journal 16, no. 4 (2017), 35-50. doi:10.11610/connections.16.4.02.

[5] Steve Rose, "The ISIS propaganda war: a hi-tech media jihad," The Guardian 7 (2014).

Uses and Gratifications Theory (UGT) is an approach that is extensively used by many people who seek specific media outfits with the aim of satisfying specified needs.[6] Historically, the UGT was applied during the Nazi Germany era; however, things have changed since that time as the only viable approach by then.[7] Seeing how it was applied in the past, ISIS grabbed on UGT and is utilizing it. On multiple occasions, ISIS has successfully manipulated and lured many young adults to join their team through social media.[8] ISIS targets younger people due to their communication and technological skills and, thus, serves its needs appropriately.

ISIS has effectively employed the UGT to propagate and recruit followers.[9] It is explainable by the UGT's distinct differences with other media effect theories approaches, which mostly focus on what the media generally does to people in return following their use. On the other hand, the UGT approach focuses on what the audience does with the media in fulfilling their wants and needs. Still, the media choices are not only limited to television, twitter, radio, snap chat, Facebook, and Instagram.[10] This model, to an extent, appears to be working in favour of ISIS in recruiting from Africa, Asia, and the Middle East countries. They are motivated by the fact that it clearly shows what kind of social media is being adopted, the necessary uses, and motivates its users to shy away from other sites available. In essence, a large number of previous works on media that targets the audiences anticipates a one-sided relationship. For instance, Magic

[6] Gina M. Chen, "Tweet this: A uses and gratifications perspective on how active Twitter use gratifies a need to connect with others," Computers in Human Behavior 27, no. 2 (2011): 755-762. doi:10.1016/j.chb.2010.10.023.

[7] *Ibid.*,755.

[8] *Ibid.*,760.

[9] Anabel Quan-Haase and Alyson L. Young, "The Uses and Gratifications (U&G) Approach as a Lens for Studying Social Media Practice," The Handbook of Media and Mass Communication Theory, 2014, 269-286. doi:10.1002/9781118591178.ch15.

[10] Alex Schmid, "Challenging the Narrative of the "Islamic State"," Terrorism and Counter-Terrorism Studies, 2015. doi:10.19165/2015.1.05.

Bullet theory that terms the audience as passive viewers with minimal response.[11] But in the case of UGT, it tries to justify the importance of comprehending the complicated relationship that exists between audience and media targeted by the ISIS group to spread their message.

Following the rise in innovation, the UGT approach seems more reliable for terrorist organizations, as it focuses on social-psychological relations with the mass media. This collaboration provides the audience with the freedom to choose the media sample that satisfies a specified need, while still giving them chances to attain affection, cognitive needs, social and personal integrative needs.[12] To expand, cognitive needs entail the desire to acquire knowledge, by the use of media. That this might just be a confirmation bias is irrelevant: it is that the audience is fed interactions in a manner that they perceive they are in charge of what they are learning. In contrast, affection needs are considerably emotional, not cognitive, and lastly, personal integrative needs are self-esteemed needs intending to attain credibility and stability.[13]

ISIS uses the UGT to its advantage by encoding messaging that would appeal to its target audience, which is mostly young elites with access to modern media platforms.[14] This indirect replication makes the audience believe it is actively participating in the ISIS project. These messages are utilized to modify how the targeted population views their actions, as they are made to believe their actions are justifiable in line with the Imam's teachings. Much like flat earthers, ISIS leads vulnerable people to

[11] Steve Rose, "The ISIS propaganda war: a hi-tech media jihad," The Guardian 7 (2014).
[12] *Ibid.*,4.
[13] Sarah Ponder and Jonathan Matusit, "Examining ISIS Online Recruitment through Relational Development Theory," Connections: The Quarterly Journal 16, no. 4 (2017), 35-50. doi:10.11610/connections.16.4.02.
[14] Nelly Lahoud, "The 'Islamic State' and al-Qaeda," Oxford Scholarship Online, 2017, doi:10.1093/acprof:oso/9780190650292.003.0002.

other vulnerable people, which amplifies their core message and gives it the look of legitimacy vis-à-vis an online community. Furthermore, this is tied into the development stages of UGT, progressing hierarchically First satisfying people's critical needs are highly recommended appearing at the base of the pyramid with essential needs, followed by more existential social needs.[15] This creates depth in the relationship and trust. Specifically, with respect to Twitter, the platform gives the audience the illusion of choosing threads and feeds friendships, but they are circular, coming back to an ISIS-controlled microcosm within the Internet. Contrary to older social media platforms like Facebook, the audience currently can hold onto the two accounts and effectively use them, so the online network needs to integrate across devices. ISIS does not just push out propaganda as an extension of analogy methods, they are interactive. It is like the difference between a movie and a video game.

ISIS applies the UGT to shape the message that it broadcasts. Many ISIS operatives have successfully lured others by displaying clips and Imams that would incite a positive reaction and feed into people's sense of justice. There are instances where ISIS showed people propaganda messages such as: "Look at the Muslims they are being killed. Look at the child, they killed his father."[16] These strategies are used to target an emotional response from their followers. By doing so, members have been brainwashed with the sentiments such as "even though we don't have guns like the enemy, we can still

---

[15] *Ibid.*,23.

[16] Ronald Tiersky, "ISIS's Deadliest Weapon Is the Idea of Heaven," RealClearWorld, Last modified September 19, 2016, https://www.realclearworld.com/articles/2016/09/19/isiss_deadliest_weapon_is_the_idea_of_heaven_112051.html.

defeat them and win."[17] This manipulation has successfully attracted candidates to join ISIS. ISIS often misquotes the Imam, which then fools a susceptible audience in believing that the war is justifiable. This clever manipulation, which does not represent any consensus within the faith, appeals to emotions of the targeted demographic to maximize recruitment. Indeed, the circulation of such clips on social media has charmed many youths (an inherently vulnerable group) who have opted to join ISIS and thus, populating the militia with not just fighters, but a generation of non-digital immigrants who can feed back into their technologically sophisticated propaganda arm. ISIS also initiated a training program through social media, broadcasting videos that demonstrate how to create improvised explosive devices. Although not directly linked to recruiting, these bomb-making videos are a necessary evolution in indoctrinating the online community. Let us take the bombing of the Boston Marathon as an example. ISIS turned their bomb-making investment into a recruiting campaign by glorifying killing and suicide. These acts introduced a susceptible population to the idolization of killing and martyring, which resulted in bolstering ISIS ranks.[18] However, because this happened through the virtual domain, it was a dissociative gateway that would then lead someone to immigrate to the Islam State. This is not to say that this was their original strategic plan that they had thought outthought sophisticated analysis. It is only to say the violence begets violence, sometimes in a very mindless way. ISIS has demonstrated its ability to take advantage of how violence can make messaging much simpler with fewer requirements to be logical or coherent; and, when combined with modern social media platforms, is an effective recruitment technique.

---

[17] Nelly Lahoud, "The 'Islamic State' and al-Qaeda." Oxford Scholarship Online, 2017, doi:10.1093/acprof:oso/9780190650292.003.0002

[18] *Ibid.*,21

ISIS and Twitter

Amid the numerous social media platforms used by ISIS to promote terror attacks, Twitter has proven to be an excellent platform when it comes to recruitment.[19] Similar to other social media platforms, Twitter has a vast audience and universal outreach with more than 1 billion subscribers. Research has shown that Twitter has an average of almost 350,000 twitter messages sent per minute and practically 500,000 tweets posted daily.[20] ISIS uses Twitter to not only disseminate their ideology but also to recruit new members, which ultimately results in a global increase in intimidation and fear. Even though Twitter cap a message at 140 characters, ISIS uses the platform effectively by depicting messages of fear and false religious doctrines. By accompanying the tweet with some well-worded comments, ISIS is capable of effectively broadcasting and appealing to a massive Twitter audience.[21] ISIS' main goal is the mass propaganda of an extremist message to the broadest receptive audience possible. ISIS Twitter reaches far exceed its published handles as their message is also supported, and retweeted by approximately thirty other online media groups. The sheer volume privileges simplicity shock over reason. For example, the al-Battar Media Group, with 32,000 followers, continually works to mobilize Twitter members to support ISIS by translating ISIS

[19] *Ibid.*,20.

[20] Jytte Klausen, "Tweeting theJihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," Studies in Conflict & Terrorism 38, no. 1 (2014): 1-22. doi:10.1080/1057610x.2014.974948.

[21] *Ibid.*,20.

releases and by independently producing media.[22] In 2014, Katz quickly demonstrated the far reach that ISIS has on twitter:

> The Billion Muslim campaign has generated over 22,000 posts within four days since its launch on June 13, 2014. On June 20, 2014, Twitter users began distributing images displaying words of encouragement or the phrases "All Eyes on ISIS" and "We are all ISIS" in Twitter posts that feature the hashtag "#AllEyesOnISIS." The hashtag now totals over 30,000 tweets." Whilst Twitter has been actively suspending many of the Isis accounts, Isis continues to have an online presence, and as this study will show, are using this to intimidate and radicalize people.[23]

ISIS effectively uses Twitter as a publicity tool to convey their messages and pass out false information to thousands of users. ISIS media broadcast uses Twitter to send out bulk messages at a higher rate with retweets to their followers.[24] Twitter acts as an amplifier that ISIS uses superbly to manipulate users in believing how good and normal it is to participate in terror activities. It is aimed at winning the hearts and minds of the younger, and highly influenceable, generation. Twitter also allows ISIS to achieve a more sustained global presence, thus extending its reach to places like Europe. In a twisted irony, this has further validated their status as a proto-state as legitimate states are forced to deal with their social media attacks, and acknowledge they are at war with them. For example, reports show that the ISIS fighters use Twitter to post beheaded photos with captions like #Wolrdcup showing that they find pleasure in their killing activities.[25] The gruesome killings of citizens from other countries forces States to take steps to curtail

---

[22] Rita Katz, "Follow ISIS on Twitter: A Special Report on the Use of Social Media by Jihadists," Latest Articles, Last modified June 26, 2014. https://news.siteintelgroup.com/blog/index.php/categories/jihad/entry/192-follow-isis-on-twitter-a-special-report-on-the-use-of-social-media-by-jihadists.

[23] *Ibid.*,5.

[24] *Ibid.*,7.

[25] WIRED, "Why ISIS Is Winning the Social Media War," WIRED, Last modified April 2016. https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/.

ISIS's social media activity, which in turn further ostracizes and solidifies the hate of ISIS' recruitment demographic.

Statics shows that ISIS has thirty media groups in addition to its overall local pages.[26] The Al-Battar media group, which has over 30,000 followers, utilizes Twitter to mobilize members in supporting ISIS. The group also goes as far as editorializing its messages, which, once again, increased the audience that could be influenced.[27] ISIS is also assisted by numerous Muslim sympathizers that are encouraging, on Twitter, young individuals to support them. Often used captions such as #AllEyesOnISIS garnered almost 30,000 retweets.[28] Despite several attempts by Twitter to suspend such terrorism accounts, ISIS has been able to grow unchecked over the internet where it can intimidate and radicalize people into joining its movement. Twitter has been undeniably a vital tool to disseminate and tailor information by ISIS.

ISIS members and supporters have been able to generate several accounts on Twitter like the famous Al-I'tisam page used to market ISIS propaganda. Moreover, many accounts such as @Nnewsi, @ShamiWitness @Minbar, @mghol1122, @alfurqan2013, and @hashtag_ISIS have transformed Twitter into an ISIS megaphone used to propagate terror and criminal offences.[29] These accounts help ISIS factions in updating its ISIS followers on their daily activities. These independent accounts are capable of continuing the spread of ISIS's message when Twitter shuts down ISIS'

---

[26] *Ibid.*,9.
[27] *Ibid.*,10.
[28] Rita Katz, "Follow ISIS on Twitter: A Special Report on the Use of Social Media by Jihadists," Latest Articles, Last modified June 26, 2014. https://news.siteintelgroup.com/blog/index.php/categories/jihad/entry/192-follow-isis-on-twitter-a-special-report-on-the-use-of-social-media-by-jihadists.
[29] *Ibid.*,23.

accounts. It is done after a close examination of the accounts used in propagating the ISIS agenda. Of all these Twitter accounts, the @ShamiWitness account has emerged as the most profitable Twitter account and has positively been able to attract over 17,000 new members. Channel four news research shows that the tweets from this account have had almost 2 million views monthly.[30]

When journalists reported that the main user of @shamiWitness, who was identified as Mehdi Masroor, had been arrested, it produced a massive online response.[31] It led to a Twitter strike with the hashtag #FreeShamiWitness circulating, making it the highest trend on twitter at that moment in time. Between #FreeShamiWitness and the lack of ability for Twitter to positively link Mehdi Masroor with the handle @shamiWitness, the account was reactivated. This was an important moment for ISIS since a lack of internet governance led to a backlash that was not effectively resolved, encouraging ISIS boldness. It was an accelerant to ISIS' recruitment campaign. Videos and pictures that play on stereotypical ideologies and show terrorism, were confusingly allowed to be transmitted through Twitter. The Twitter structure enables terrorist groups like ISIS, through an enormous user-based platform, the ability to target the influenceable population, especially the youth who tend to retweet such posts, regardless to what extent they support the organization.

Extremist groups are viewed to be very active advocates when it comes to the public Internet and online publicity. It is a standard method used by terrorist groups, like

---

[30] Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," Studies in Conflict & Terrorism 38, no. 1 (2014): 1-22, doi:10.1080/1057610x.2014.974948.
[31] *Ibid.*,22.

ISIS, to entice and employ their new possible members.[32] Cyberspace, especially Twitter, is a much more comfortable and convenient method to communicate with a larger group of people. Terrorist groups like ISIS take advantage of this technological improvement to motivate their followers and lure them into becoming one of them. Twitter has, therefore, immensely helped ISIS in the radicalization and transformation of individuals. The change in the radicalization of the newest recruits was created by forgetting the recruit's prior beliefs on terrorism. It uses Twitter to feed members with massive visual and textual info that portrays the act of terrorism as a fun activity to indulge. Some of the popular hashtags are #IslamDevleti, #PKK, #Iraq. It is at heart a disturbing modern version of Romanticism. Violent murders and execution recordings are posted on Twitter account to incite ISIS adversaries in a race to the ethical bottom, as well as to recruit followers from other parts of the world who only tangentially feel the realities of war at its most horrific.

ISIS and Facebook

Facebook is a platform that has a wide range of uses when it comes to terrorism. Facebook is not only used for donation solicitation but also to recruit sympathizers and followers. Technology has been the cornerstone in enhancing message delivery, which terrorist organizations have continued to use to obtain information regarding different users.[33] After accessing the user's information, the terrorist organization, such as ISIS, will contact individuals who have shown interest or passion on the pages to join terror organizations. Generally, terrorist recruiters have preferred to seek recruits rather than

[32] Gina M. Chen, "Tweet this: A uses and gratifications perspective on how active Twitter use gratifies a need to connect with others," Computers in Human Behavior 27, no. 2 (2011): 755-762, doi:10.1016/j.chb.2010.10.023.

[33] Natalia Macrynikola and Regina Miranda, "Active Facebook use and mood: When digital interaction turns maladaptive," Computers in Human Behavior 97 (2019), 271-279, doi:10.1016/j.chb.2019.02.012.

sitting back and wait for them to join.[34] Most of the recruitment tools used by terrorists have integrated anti-state propaganda and twisted religious orders. In this case, terrorists have led their sympathizers to secret chat rooms on the darknet where they are provided training manuals. Facebook also enables communication with the recruits to instruct them to travel and join the militia in Iraq and Syria.[35]

Facebook, like other social media platforms, is borderless and can attract a large number of people from all parts of the world. To achieve this, an individual would create a personal profile or a page and upload his pictures accompanied by his contact information. Afterwards, they would try to create a connection with other Facebook users with the same interest creating a group of people. It is not exempting individuals and organization with ill motives like ISIS, who uses that platform to attract people into Islamic extremist groups. ISIS has used Facebook to promote terrorism through comments, writings, and propaganda videos that brainwashes people. It modifies the target individual, which starts to develop an interest in extreme Islamic religious teachings that radicalized its believers.[36]

The extremist ideology is tailored to the targeted audience so that it only portrays the facets that the group would find attractive. For example, terrorist groups have continuously posted videos titled learning self-defence. In reality, these videos are solely meant to radicalize people by teaching them how to use or assemble explosive weapons. Other clips orient people on how to hack as well as encrypt deadly viruses.[37] Upon identification of the interested parties, ISIS tailors further their content, ensuring the use

[34] *Ibid.*,274.
[35] *Ibid.*,275.
[36] *Ibid.*,277.
[37] *Ibid.*,279.

of modern marketing concepts of repetition and reinforcement through a mix of propaganda, profiling terrorist acts, and persuasive talks presented by supposed Islamic authorities.[38] It generally culminates with showing the future recruits videos of training sessions conducted at its terrorist training camps and by promising some incentives upon recruitment.[39] Here is an example of a recruiting message that targets a Canadian audience:

> I am your brother in Islam here in Syria. I originally come from Canada, [and while panoramic shots of a snow-covered Canadian mountain range with children playing hockey in the foreground appear on-screen he continues], before Islam I was like any other regular Canadian, I watched hockey, I went to the cottage in the summertime, I loved to fish . . . I liked the outdoors; I liked sports. [He goes on to urge other Canadians Muslims not to continue living in a land where they are oppressed, implying that even normal people like him are capable of making the trip to Syria and are accepted once they arrive].[40]

Facebook radicalization has been used as a method by ISIS to transform followers into more violent extremist individuals. It maximized the use of propaganda in encoded video or writing to effectively perused susceptible people. Facebook internal algorithms, in turn, reinforce the echo chamber effect, and synthesizing groups with historic grievances whoever unrelated they are. In the U.S, ISIS has continuously targeted African Americans because they see them as oppressed, vulnerable and influenceable, and by following their situations, ISIS can capitalize on mixed messaging. ISIS also employs propaganda that tends to radicalize black people against a white population and

---

[38] Christina Schori Liang, "Cyber Jihad: understanding and countering Islamic State propaganda," GSCP Policy Paper 2, no. 4 (2015): 1-12.

[39] Dr.P., P.M. Vishnu Balasubramanian and Sushmitha Sidharth, "Social Media as a Recruitment Tool," Bonfring International Journal of Industrial Engineering and Management Science 6, no. 3 (2016), 108-110. doi:10.9756/bijiems.7468.

[40] Richard N. Landers and Gordon B. Schmidt. "Social Media in Employee Selection and Recruitment: An Overview," Social Media in Employee Selection and Recruitment, 2016, 3-11. doi:10.1007/978-3-319-29989-1-1.

especially a majority white authority.[41] It is executed through the dissemination of fake mythical relationships that supposedly link African Americans' reality to that of the Islamic religion. This in itself, is not a new tactic and goes back to Malcom X and the Nation of Islam, but social media's ability to make global connections is. ISIS' goal is to create a pool of Americans that could be used to conduct terror acts on American soil.

Africa being a developing continent, faces several challenges, not limited to dictatorship, high unemployment, and technological latency. Terrorist groups have primarily taken advantage of these existing obstacles to convert and recruit Africans into ISIS. It has psychologically shaped terrorists to be fighters for justice by those of extreme Islamic believes.[42] ISIS uses Facebook to attract many youths by falsely presenting the benefits of joining such groups, which include financial stability, and a fight for justice. These powerful messages, coupled with socio-economic pressures, are increasingly viewed as the only option available. The recruits are trained and made to execute violent and sometimes deadly actions in Africa and other parts of the world.[43] For example, the 1998 bombing of the United States embassy in Nairobi, Kenya by Africans ISIS believers was executed to demonstrate their rebellion against the United States' operations in the Muslim states of Iraq.[44] The operation was mostly planned and coordinated through Facebook.

---

[41] Vernon Silver, and Sarah Frier, "Bloomberg," Bloomberg - Are You a Robot?, Last modified May 10, 2018, https://www.bloomberg.com/news/articles/2018-05-10/terrorists-creep-onto-facebook-as-fast-as-it-can-shut-them-down.

[42] Donald Holbrook, "A critical analysis of the role of the internet in the preparation and planning of acts of terrorism," Dynamics of Asymmetric Conflict 8, no. 2 (2015): 121-133.

[43] *Ibid.*, 122.

[44] Jason Burke, "Africa Embassy Bombings: Attacks That Propelled Bin Laden Into the Limelight," The Guardian, Last modified November 29, 2017, https://www.theguardian.com/world/2015/jan/20/africa-embassy-bombings-osama-bin-laden-kenya-tanzania-al-qaida.

THEMES

Branding

ISIS has succeeded in recruiting relevant capabilities to the organization from across the world using social media. It is believed that in 2017, ISIS has more than 30,000 members from at least 100 countries.[45] Social media has enabled the transfer of information from one country to another with little to no carrying cost. ISIS seized the opportunity to use social media to spread its propaganda, false religious information, recruit new soldiers, and incite the public against various forms of authority. ISIS employs a multitude of social media platforms such as Twitter, Facebook, YouTube, and online magazines like Dabiq, supported by countless chat groups.[46] ISIS is waging war on the ground, online, and in cyberspace. Over the years, extremist groups have strengthened their communication strategies by recruiting highly trained individuals, focusing on recruits with computer knowledge and information technology skills.[47] The war in the cyber domain is centrally managed and executed by specialists within the organization under what could be termed as an information ministry.[48] This department has succeeded in producing high-quality videos, speeches, images, and radios shows which are typically distributed through a wide range of authorized news agencies like al-Hayat Media Center, al-Bayan, and Furqan.[49] ISIS is also using official news agencies to

---

[45] Steve Rose, "The ISIS propaganda war: a hi-tech media jihad." The Guardian 7 (2014).

[46] Clara Pellerin, "Communicating terror: An Analysis of ISIS Communication Strategy," Science Po Kuwait Program, http://www.sciencespo.fr/psia/sites/sciencespo.fr.psia/files/PELLERIN_Clara_KSP_Paper_Award.pdf.

[47] *Ibid.*,22.

[48] *Ibid.*,24.

[49] Nathan K Schneider, "ISIS and Social Media: The Combatant Commander's Guide to Countering ISIS's Social Media Campaign," 2015, Last modified June 16, 2014, doi:10.21236/ada621060.

achieve legitimacy and spread its influence beyond the Middle East borders. To strengthen its cause towards legitimacy, ISIS is imitating the logos of popular and reputable sources such as Al Jazeera. In October 2014, ISIS created the Al-Zora Foundation, which they use as a new wing of social media. Finally, ISIS develop a smartphone application that is widely used by its followers and is known as Dawn of Glad Tidings.[50]

Recruiting the Youth

There are numerous documented cases of teenagers being stopped as they are actively trying to leave their countries to join ISIS.[51] Most of these young people admitted to having been recruited through social media platforms. For instance, Shannon Conley, nineteen years old, was stopped at an airport in the United States by the Federal Bureau of Investigation. She was convinced that her nursing skills could help the organization. Shannon was lured by a Tunisian recruiter who promised to marry her.[52] Another teenager named Mohammed Hamzah Khan was stopped in Chicago with his younger sister and brother. According to Khan, the government of the United States was using their taxes to kill innocent Muslims across the borders. Therefore, Khan, with his young siblings, decided to join ISIS to avoid the killing of Muslims through the use of their taxes.[53] In October 2014, three young ladies from Germany ages 17, 16, and 15 were reportedly stopped on their way to join the ISIS group in Syria.[54] These are just a few cases that demonstrate the reach that ISIS has and its ability to influence the mind of

[50] J.M. Berger, "How ISIS Games Twitter," The Atlantic, Last modified June 16, 2014. https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.
[51] *Ibid.*,6.
[52] *Ibid.*,6.
[53] Ben Connable, Natasha Lander and Kimberly Jackson, "Beating the Islamic State: Selecting a New Strategy for Iraq and Syria," 2017. doi:10.7249/rr1562.
[54] *Ibid.*,23.

the younger generation. ISIS skillfully used social media to lure these people through propaganda, incitement, and false religious messages. One of the messages that ISIS utilize to propagate their false religious intentions is

> For an Islamist fundamentalist, Heaven is a real place, a Garden full of sensual delights. For example, take the famous claim that in Heaven, a deserving Muslim will enjoy the company of 72 virgins. This is nowhere mentioned in the Qoran. It is found in a fanciful hadith by Ibn Kathir, writing in the 14th century, hundreds of years after prophet Mohammed's death: "Prophet Mohammed was heard saying, 'The smallest reward for the people of paradise (the meaning of course only men) is an abode where are 80,000 servants and 72 wives, over which stands a dome decorated with pearls, aquamarine, and ruby…'" Innumerable such tall tales appear throughout the history of Islamic commentary.[55]

In 2015, then-President Obama with Secretary of State John Kerry, publicly admitted that ISIS group is using propaganda to target, lure and recruit young people across the world.[56] In his speech, President Obama emphasizes the need and urgency to shut down all the machinery, such as social media, as well as the propaganda, which is being used by terrorists to recruit young adults into dangerous groups.[57] In a notable address made in February 2015 at the Washington summit to counter violent extremist, President Obama stated that:

> Terrorist groups such as ISIS and al-Qaeda, deliberately target their propaganda in the hopes of reaching and brainwashing young Muslims, especially those who may be disillusioned or wrestling with their identity. The high-quality videos, the online magazines, the use of social media,

---

[55] Ronald Tiersky, "ISIS's Deadliest Weapon Is the Idea of Heaven," RealClearWorld, Last modified September 19, 2016, https://www.realclearworld.com/articles/2016/09/19/isiss_deadliest_weapon_is_the_idea_of_heaven_112051.html.

[56] Emma L. Briant, "Propaganda 'boundaries' and the extended apparatus," Propaganda and counter-terrorism, 2015, doi:10.7765/9781847799630.00007.

[57] FBI: ISIS message resonating with young people from U.S., West, CBS NEWS (Mar. 5, 2015, 8:15 PM), http://www.cbsnews.com/news/isis-targeting-young-people-from-u-s-western-countries-as-recruits.

terrorists Twitter accounts, it's all designed to target today's young people online.[58]

Love Versus Hate

ISIS produces numerous videos that air propaganda messages, which are intended to portray their group as the most dangerous and competent group on the battlefield. These videos are of high-quality, and in most cases, incorporate slow-motion scenes, short dialogue, and montages.[59] The content of the video consists typically of mass shootings, beheadings, and/or torturing of the considered enemies within their self-proclaimed territories. These videos depict a dedicated group, a brotherhood, that shows inclusion and equality.[60] These videos also encourage the mass to support ISIS' cause, especially the fight against a common enemy. They also bear the message of radicalization of the international community so that victory in the Caliphate can be achieved.[61] ISIS has ingeniously manipulated its message to show two simultaneous vision, one of hate and one of love. The videos are used to provoke or frighten their adversaries and at the same time to recruit sympathizers from different parts of the world.

The widespread distribution of such videos has succeeded in persuading young people, both men and women, that the Caliphate is the idealistic world, especially to those that are part of the cause. The ISIS love and hate messages have successfully motivated a large number of individuals to migrate from their respective countries to the

---

[58] Kathy Gilsinan, "Why ISIS's Power on Twitter and Facebook Is Overrated," The Atlantic, Last modified February 23, 2015, https://www.theatlantic.com/international/archive/2015/02/is-isiss-social-media-power-exaggerated/385726/.

[59] Steve Rose, "The ISIS propaganda war: a hi-tech media jihad." The Guardian 7 (2014).

[60] Richard N. Landers and Gordon B. Schmidt, "Social Media in Employee Selection and Recruitment: An Overview," 3-11.

[61] Kathy Gilsinan, "Why ISIS's Power on Twitter and Facebook Is Overrated." The Atlantic, Last modified February 23, 2015, https://www.theatlantic.com/international/archive/2015/02/is-isiss-social-media-power-exaggerated/385726/

ISIS-controlled region for the sake of Allah.[62] In ISIS, Al-Hayat Media, as mentioned earlier, is responsible for the video production and its primary duty is to lure the non-Arabic speaking population.[63] Additionally, Al-Hayat Media produces its love and hate videos in numerous languages such as English and Turkish, to cover a wide range of people and increase its reach.

CONCLUSION

This paper has demonstrated ISIS's proficiency with social media and the extraordinary success that ISIS has had to attract new followers and recruits. ISIS's rise and successes in battle are inseparable from their strategic communications and recruitment. The casualties they have suffered and the enemies they have created through their abhorrent version of Islam would be unsustainable without social media providing a pool of new frantic fighters. Additionally, the point was made that ISIS has not only solely attracted recruits but has also used social media to grow terrorists through modern marketing and social media techniques. It demonstrated that the materials, religious messages, and social aspects were the most effective recruiting themes but were successful because they were carried upon a medium that allows the identification and isolation of vulnerable targets. The analysis was done through an evaluation of the various platforms that ISIS utilizes to shape, recruit, and brainwash recruits. It then shifted to a detailed evaluation of the common themes that ISIS utilizes to recruit its targeted individual include branding, recruiting the youths and love versus hate.

---

[62] H. Gil de Zúñiga, T. Diehl, B. Huber and J. Liu, "Personality Traits and Social Media Use in 20 Countries: How Personality Relates to Frequency of Social Media Use, Social Media News Use, and Social Media Use for Social Interaction," Cyberpsychology, Behavior, and Social Networking 20, no. 9 (2017), 540-552. doi:10.1089/cyber.2017.0295.

[63] Martin Rudner, "Electronic Jihad: The Internet as Al Qaeda's Catalyst for Global Terror," Studies in Conflict & Terrorism 40, no. 1 (2017): 10-23.

Social media has transformed terrorism forever. ISIS successfully exploited the vast data associated with social media and the interconnectivity of the internet to advance their political and military agenda. The essential organizational demands such as recruitment, publicity, and funding are achieved conveniently by the click of a button. With the use of technology, the traditional recruit pool has been vastly extended. ISIS recruiters can now reach, manipulate, recruit, and instruct candidates without leaving their houses. ISIS uses social media to launch its propaganda and can reach unimaginable potential recruits across the borders. It is important to note that the spread of such information on social media is broadcast without restrictions or regulatory oversight.

ISIS maximizes the use of online platforms through multiple users, which allows them to mass discriminate tailored messages to social media, chat applications, and other websites. This technique has extended the reach of ISIS significantly. Technology is continuously evolving and can be easily manipulated to advance good and evil causes. Social media is providing unprecedented open access to lure young, malleable individuals directly as well as influencing new supporters through hashtags, messaging, and much more. To date, efforts to impede the ISIS recruiting machine on social media have proven relatively ineffective. It is therefore imperative that governments and the private sector dedicate more efforts to counter the use of social media by such groups.

The analysis presented in this paper is explicit, ISIS favours the uses of social media to influence and lure more members to join their team. For instance, the use of twitter to discriminate false religious messages has been used extensively to lure different members to join the ISIS across the world. Facebook links and messages are also other crucial platforms that the group has used to lure many members to join the group

worldwide. In many instances, ISIS twists religious messages such as *the deadly heaven messages of the Promised Land* and *the 72 Virgins* to entice followers to join. They have even employed themes such as violence branding, youth recruitment, and love versus hate, through the use of selective chapters to foster their radicalization message.

BIBLIOGRAPHY

Balasubramanian, Dr.P., P.M. Vishnu, and Sushmitha Sidharth. "Social Media as a Recruitment Tool." Bonfring International Journal of Industrial Engineering and Management Science 6, no. 3 (2016), 108-110. doi:10.9756/bijiems.7468.

Berger, J.M. "How ISIS Games Twitter." The Atlantic. Last modified June 16, 2014. https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.

Briant, Emma L. "Propaganda 'boundaries' and the extended apparatus." Propaganda and counter-terrorism, 2015. doi:10.7765/9781847799630.00007.

Burke, Jason. "Africa Embassy Bombings: Attacks That Propelled Bin Laden Into the Limelight." The Guardian. Last modified November 29, 2017. https://www.theguardian.com/world/2015/jan/20/africa-embassy-bombings-osama-bin-laden-kenya-tanzania-al-qaida.

Chen, Gina M. "Tweet this: A uses and gratifications perspective on how active Twitter use gratifies a need to connect with others." Computers in Human Behavior 27, no. 2 (2011): 755-762. doi:10.1016/j.chb.2010.10.023.

Connable, Ben, Natasha Lander, and Kimberly Jackson. "Beating the Islamic State: Selecting a New Strategy for Iraq and Syria." 2017. doi:10.7249/rr1562.

FBI: ISIS message resonating with young people from U.S., West, CBS NEWS (Mar. 5, 2015, 8:15 PM), http://www.cbsnews.com/news/isis-targeting-young-people-from-u-s-western-countries-as-recruits/.

Gil de Zúñiga, H., T. Diehl, B. Huber, and J. Liu. "Personality Traits and Social Media Use in 20 Countries: How Personality Relates to Frequency of Social Media Use, Social Media News Use, and Social Media Use for Social Interaction." Cyberpsychology, Behavior, and Social Networking 20, no. 9 (2017), 540-552. doi:10.1089/cyber.2017.0295.

Holbrook, Donald. "A critical analysis of the role of the internet in the preparation and planning of acts of terrorism." Dynamics of Asymmetric Conflict 8, no. 2 (2015): 121-133.

Katz, Rita. "Follow ISIS on Twitter: A Special Report on the Use of Social Media by Jihadists." Latest Articles. Last modified June 26, 2014. https://news.siteintelgroup.com/blog/index.php/categories/jihad/entry/192-follow-isis-on-twitter-a-special-report-on-the-use-of-social-media-by-jihadists.

Klausen, Jytte. "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq." Studies in Conflict & Terrorism 38, no. 1 (2014): 1-22. doi:10.1080/1057610x.2014.974948.

Landers, Richard N., and Gordon B. Schmidt. "Social Media in Employee Selection and Recruitment: An Overview." Social Media in Employee Selection and Recruitment, 2016, 3-11. doi:10.1007/978-3-319-29989-1_1.

Liang, Christina Schori. "Cyber Jihad: understanding and countering Islamic State propaganda." GSCP Policy Paper 2, no. 4 (2015): 1-12.

Pellerin, Clara. "Communicating terror: An Analysis of ISIS Communication Strategy." Science Po Kuwait Program. Last modified 2016. http://www.sciencespo.fr/psia/sites/sciencespo.fr.psia/files/PELLERIN_Clara_KSP_Paper_A ward.pdf.

Quan-Haase, Anabel, and Alyson L. Young. "The Uses and Gratifications (U&G) Approach as a Lens for Studying Social Media Practice." The Handbook of Media and Mass Communication Theory, 2014, 269-286. doi:10.1002/9781118591178.ch15.

Rose, Steve. "The ISIS propaganda war: a hi-tech media jihad." The Guardian 7 (2014).

Rudner, Martin. "Electronic Jihad": The Internet as Al Qaeda's Catalyst for Global Terror." Studies in Conflict & Terrorism 40, no. 1 (2017): 10-23.

Schmid, Alex. "Challenging the Narrative of the "Islamic State"." Terrorism and Counter-Terrorism Studies, 2015. doi:10.19165/2015.1.05.

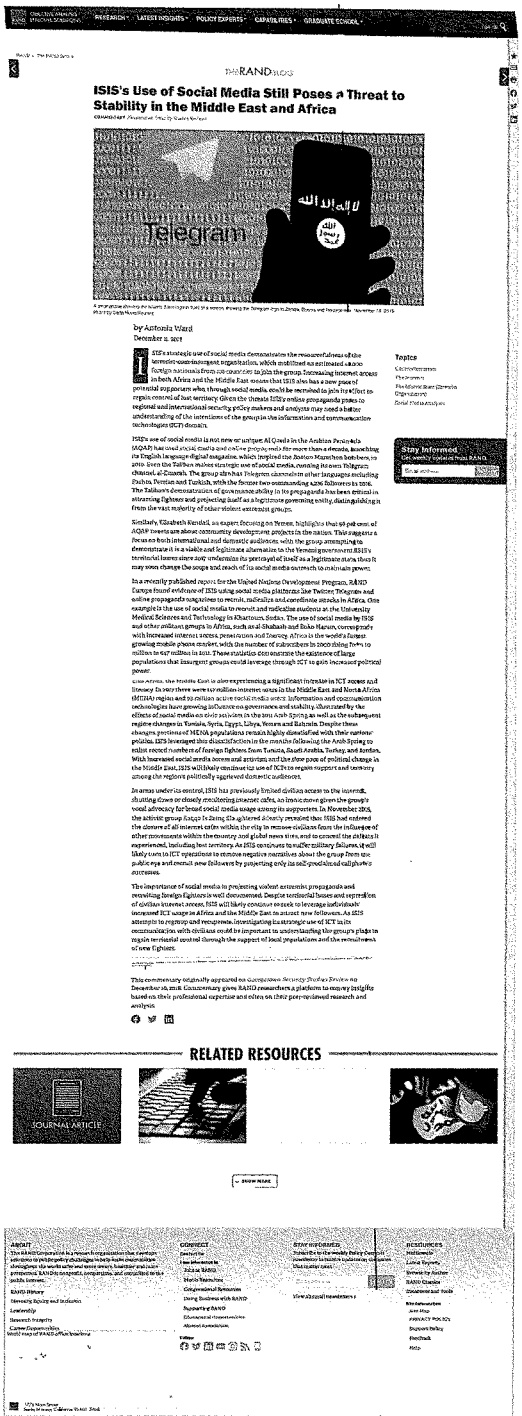
Schneider, Nathan K. "ISIS and Social Media: The Combatant Commander's Guide to Countering ISIS's Social Media Campaign." 2015. doi:10.21236/ada621060.

Silver, Vernon, and Sarah Frier. "Bloomberg." Bloomberg - Are You a Robot?. Last modified May 10, 2018. https://www.bloomberg.com/news/articles/2018-05-10/terrorists-creep-onto-facebook-as-fast-as-it-can-shut-them-down.

Tierney, Ronald. "ISIS's Deadliest Weapon Is the Idea of Heaven." RealClearWorld, Last modified September 19, 2016. https://www.realclearworld.com/articles/2016/09/19/isiss_deadliest_weapon_is_the_idea_of_heaven_112051.html.

Ward, Antonia. "ISIS's Social Media Use Poses a Threat to Stability in the Middle East and Africa." RAND Corporation Provides Objective Research Services and Public Policy Analysis | RAND. Last modified December 11, 2018. https://www.rand.org/blog/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html.

WIRED. "Why ISIS Is Winning the Social Media War." WIRED. Last modified April 2016. https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/.



RESEARCH · LATEST INSIGHTS · POLICY EXPERTS · CAPABILITIES · GRADUATE SCHOOL

THE RAND BLOG

ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa

A propaganda picture by Islamic State group fighters showing the Telegram logo in Arabic. Photo by Reuters. November 18, 2015.

by Antonia Ward
December 9, 2017

ISIS's strategic use of social media demonstrates the resourcefulness of the terrorist-cum-insurgent organization, which mobilized an estimated 40,000 foreign nationals from 110 countries to join the group. Increasing internet access in both Africa and the Middle East means that ISIS also has a new pool of potential supporters who, through social media, could be recruited to join its effort to regain control of lost territory. Given the threats ISIS's online propaganda poses to regional and international security, policy makers and analysts may need a better understanding of the intentions of the group in the information and communication technologies (ICT) domain.

ISIS's use of social media is not new or unique. Al Qaeda in the Arabian Peninsula (AQAP) has used social media and online propaganda for more than a decade, launching its English language digital magazine, which inspired the Boston Marathon bombers, to pro-Given the Taliban makes strategic use of social media, running its own Telegram channel, al-Emarah. The group also has Telegram channels in other languages including Pashto, Persian and Turkish, with the former two commanding 4,000 followers in 2016. The Taliban's demonstration of governance ability in its propaganda has been critical in recruiting fighters and projecting itself as a legitimate governing entity, distinguishing it from the vast majority of other violent extremist groups.

Kimberly Elizabeth Kendall, an expert focusing on Yemen, highlights that 98 percent of AQAP tweets are about community development projects in the nation. This suggests a focus on both international and domestic audiences, with the group attempting to demonstrate it is a viable and legitimate alternative to the Yemeni government. ISIS's territorial losses since 2017 undermine its portrayal of itself as a legitimate state, thus it may soon change the scope and reach of its social media outreach to maintain power.

In a recently published report for the United Nations Development Program, RAND Europe found evidence of ISIS using social media platforms like Twitter, Telegram and online propaganda magazines to recruit, radicalize and coordinate attacks in Africa. One example is the use of social media to recruit and radicalize students at the University Medical Sciences and Technology in Khartoum, Sudan. The use of social media by ISIS and other militant groups in Africa, such as al-Shabaab and Boko Haram, corresponds with increased internet access penetration and fluency. Africa is the world's fastest-growing mobile phone market, with the number of subscribers in 2000 rising from 10 million to 647 million in 2012. These statistics demonstrate the existence of large populations that insurgent groups could leverage through ICT to gain increased political power.

Like Africa, the Middle East is also experiencing a significant increase in ICT access and literacy. In 2017 there were 130 million internet users in the Middle East and North Africa (MENA) region and 70 million active social media users. Information and communication technologies have growing influence on governance and stability, illustrated by the effects of social media on civil activism in the 2011 Arab Spring, as well as the subsequent regime changes in Tunisia, Syria, Egypt, Libya, Yemen and Bahrain. Despite these changes, portions of MENA populations remain highly disenfranchised with their current politics. ISIS leveraged this disaffection in the months following the Arab Spring to enlist record numbers of foreign fighters from Tunisia, Saudi Arabia, Turkey, and Jordan. With increased social media access and activism, and the slow pace of political change in the Middle East, ISIS will likely continue its use of ICTs to regain support and territory among the region's politically aggrieved domestic audiences.

In areas under its control, ISIS has previously limited civilian access to the internet, shutting down or closely monitoring internet cafés, as Iraq is now given the group's vocal advocacy for broad social media usage among its supporters. In November 2015, the activist group Raqqa Is Being Slaughtered Silently revealed that ISIS had entered the homes of all internet cafés within the city to remove civilians from the influence of other movements within the country and global news sites, and to control the dialogue it experienced, including lost territory. As ISIS continues to suffer military failures, it will likely turn to ICT operations to remove negative narratives about the group from the public eye and recruit new followers by projecting only its self-proclaimed caliphate's successes.

The importance of social media in projecting violent extremist propaganda and recruiting foreign fighters is well documented. Despite territorial losses and repression of civilian internet access, ISIS will likely continue to seek to leverage individuals' increased ICT usage in Africa and the MENA East to attract new followers. As ISIS attempts to regroup and reorganize, investigating its strategic use of ICT in its communication with civilians could be important to understanding the group's plans to regain territorial control through the support of local populations and the reconstitution of new fighters.

This commentary originally appeared on *Cyberwarzone Security-Studies Review* on December 10, 2017. Commentary gives RAND researchers a platform to convey insights based on their professional expertise and relies on their peer-reviewed research and analysis.

Topics
Cyberterrorism
Cyberwarfare
Middle East (General)
Organizations
Social Media Analytics

Stay Informed
Get weekly updates from RAND

Email address

RELATED RESOURCES

SHOW MORE

Military Cyber Affairs

Volume 1 | Issue 1 Article 4

January 2016

The Islamic State's Use of Online Social Media

Lisa Blaker
University of Maryland, Baltimore County, Blak3@umbc.edu

The Islamic State's Use of Online Social Media

LISA BLAKER, University of Maryland, Baltimore County

1. INTRODUCTION

The Islamic State of Iraq and Syria (ISIS) has made great use of the Internet and online social media sites to spread its message and encourage others, particularly young people, to support the organization, to travel to the Middle East to engage in combat—fighting side-by-side with other jihadists, or to join the group by playing a supporting role—which is often the role carved out for young women who are persuaded to join ISIS. The terrorist group has even directed sympathizers to commit acts of violence wherever they are when traveling to the Middle East isn't possible. ISIS propaganda is now more frequently aimed at Westerners and more specifically aimed at the "Millennial generation."

Clearly, social media has proven to be an extremely valuable tool for the terrorist organization and is perfectly suited for the very audience it's intending to target. According to Pew Research Center's Social Networking Fact Sheet, 89% of adults aged 18 - 29 use social media"[1] Platforms such as Facebook and Twitter, and even YouTube, allow ISIS propaganda to reach across the globe in real time. Increasingly, ISIS' posts to Internet sites include sophisticated, production-quality video and images that incorporate visual effects.

What messages from jihadists induce young Westerners to become involved with the terrorist group? What convinces young people from Europe, Australia, Canada, and the United States—many who are technically runaways, still in their teens—to leave their homelands to join ISIS on the battlefield? What risks does a home country face when its nationals communicate and establish relationships with members of ISIS? Can the jihadist social network propaganda machine be shut down, and weighing all factors, is stopping ISIS rhetoric on the Internet the best course of action? This paper explores these and other questions related to terrorist groups' utilization of social media.

2. A PERVASIVE SOCIAL MEDIA CAMPAIGN

Just this past February, former National Security Council staffer Hillary Mann Leverett said that each day, 90,000 pro-ISIS messages were posted on social media. Reporting for the *Tampa Bay Times*, Jon Greenberg did further research on that figure—*90,000*—wondering how exactly that number was arrived at and concluded it was probably not unreasonable.

> While the exact source of that figure is a bit unclear, one independent researcher has data that point to a much higher number. There could be as many as 200,000 pro-ISIS tweets a day. That includes re-tweets and some generated by computer programs.[2]

[1] Pew Research Center, "Social Networking Fact Sheet," January 2014. Accessed April 23, 2015. http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/

[2] Jon Greenberg, "Does the Islamic State Post 90,000 Social Media Messages Each Day?" *Tampa Bay Times*, February 19, 2015. Accessed April 21, 2015. http://www.politifact.com/punditfact/statements/2015/feb/19/hillary-mann-leverett/cnn-expert-islamic-state-posts-90000-social-media-/

Recently the CEO of Twitter and other Twitter employees reported receiving death threats from ISIS. These threats resulted from Twitter revoking accounts that were used by the terrorist organization to spread their views and encourage violence against Westerners.[3] Because these threats were publicized just this past fall, Twitter's efforts to thwart ISIS by taking down accounts may seem like a fairly recent development. Actually, though, Twitter had been shutting down accounts tied to terrorists for more than a year.

In September 2013, at least 4 militants of Al-Shabaab, a Somalia al-Qaeda ally, attacked an upscale shopping mall in Nairobi. Shortly after the gunmen stormed the mall—shooting civilians and reportedly using grenades—the terrorists began "live-tweeting the carnage" from within the mall.[4] Twitter quickly shut down that account, but almost immediately another Twitter account opened which purportedly was also operated by the militants. This happened repeatedly for days—with a new Twitter account being opened by the group (or someone posing as their spokesperson) as soon as the one before was shut down. At the time, Twitter declined to discuss its specific reasoning for deactivating the Twitter accounts.

While committed to providing a forum for free speech, Twitter Rules[5] currently include the following restrictions:

- **Violence and Threats:** You may not publish or post threats of violence against others or promote violence against others.
- **Unlawful Use:** You may not use our service for any unlawful purposes or in furtherance of illegal activities. International users agree to comply with all local laws regarding online conduct and acceptable content.

Clearly terrorist activity violates these terms.

Even if Twitter itself didn't take down accounts associated with ISIS and other terrorist organizations, it's possible that Anonymous, the loosely organized hacking group, would. In February of 2015, Anonymous took credit for shutting down 800 ISIS accounts on Twitter and Facebook. Though Anonymous took credit, when the supposed hacked accounts were accessed, a message was displayed indicating that they were suspended or unavailable. It's possible that Anonymous reported the noncompliant content to Twitter and Facebook, and the social media sites took action to deactivate the accounts on their own. "They often rely on complaints from others..."[6] Some speculate that Twitter's going public in November 2013 put additional pressure on the firm to remove accounts of suspected terrorist organizations because, as a publicly traded company, it must answer to its shareholders.

---

[3] Annabel Grossman, "Twitter CEO Reveals ISIS Has Threatened to Kill Him After the Site Shut Down Jihadist Accounts," *DailyMail.com*, October 10, 2014. Accessed April 17, 2015. http://www.dailymail.co.uk/news/article-2787735/twitter-ceo-reveals-isis-threatened-kill-site-shut-jihadist-accounts.html#ixzz3XaWERpVB

[4] Brian Reis, "Twitter's Terrorist Policy," *The Daily Beast*, September 24, 2013. Accessed April 16, 2015. http://www.thedailybeast.com/articles/2013/09/24/twitter-s-terrorist-policy.html

[5] "The Twitter Rules," n.d. Accessed April 17, 2015. https://support.twitter.com/articles/18311-the-twitter-rules#

[6] Alanna Petroff, "Hundreds of ISIS Social Media Accounts Shut Down," *CNN Money*, February 10, 2015. Accessed April 16, 2015. http://money.cnn.com/2015/02/10/technology/anonymous-isis-hack-twitter/

3. MASTERFUL SELF-PROMOTION

The ISIS propaganda wing, al-Hayat, continues to mass-produce slick videos that mimic Hollywood action films and music videos and are obviously targeted to young Westerners. The videos often include music with lyrics translated into English and a number of European languages. More recent videos feature English-speaking jihadists. Notes Sean Heuston, a professor of English and film studies at The Citadel who has written about extremist video propaganda, "It's actually surprising how contemporary and hip-looking some of these things are, especially considering the fact that the messages that they are promoting are essentially medieval."[7] It's quite evident that the audiences these images are intended to appeal to are Millennials from the West.

Some believe that a German national and former rapper, Denis Cuspert, is a main contributor to the production of these videos as he would have been exposed to high-end production techniques during his music career as rapper, Deso Dogg. Leaving his music career after converting to Islam, Cuspert joined ISIS in 2012. The U.S. State Department declared Cuspert to be an international terrorist, "...Cuspert is 'emblematic of the type of foreign recruit' ISIS seeks, has been a 'willing pitchman' for the organization's 'atrocities' and as such been officially designated as a 'foreign terrorist fighter and operative'..."[8]

Some Twitter postings may seem at first glance to be nonthreatening and perhaps could even be considered constructive. For example, one Twitter posting announced the opening of schools in the city of Raqqa, Syria (considered the capital of the Islamic State) for English speaking children; these schools promised education for both boys and girls. Opportunities for full- and part-time teachers were available at the schools as well. The ISIS flag prominently pictured on the announcement along with the heading "ATTENTION ENGLISH SPEAKING MUHAJIROON!" however, make the message far more ominous. For school children 6 to 14 years old, "...lessons taught in English are Aqeedah, Hadith, Seerah, Fiqh, Thabiyyah, Jihadiyyah, Maths and English Language."[9]

4. THE SPOILS OF RECRUITMENT

Estimates are that more than 3,000 nationals from Western nations have migrated to ISIS-controlled territory in support of the extremists. The Internet and, more specifically, social media have allowed ISIS, despite the distance, to connect with thousands of people throughout the world. Associations established on social networks can progress to one-on-one communication using other "chat" services such as ChatSecure, TextSecure, and Redphone.[10]

---

[7] Bruce Wallace, "ISIS Has Mastered High-end Video Production in Its New Propaganda Wing," *PRI's World*, September 11, 2014. Accessed April 25, 2015. http://www.pri.org/stories/2014-09-11/isis-has-mastered-high-end-video-production-its-new-propaganda-wing/

[8] Andy Eckardt, "Denis Cuspert, AKA 'Deso Dog,' Named by U.S. as ISIS Terrorist," *NBCNews*, February 10, 2015. Accessed April 25, 2015. http://www.nbcnews.com/storyline/isis-terror/denis-cuspert-aka-deso-dogg-named-u-s-isis-terrorist-n303456

[9] "Now, Islamic State Opens Two English Schools in Syria's Raqqa," *In.com*, Last updated February 24, 2015. Accessed April 11, 2015. http://www.in.com/news/ipl/now-islamic-state-opens-two-english-schools-in-syrias-raqqa-53123741-in-1.html

[10] "ISIS Follower On Twitter Warns Against Using Kik Messenger Service 'When Chatting About Sensitive Jihadi Stuff,' Recommends Other Technologies," *The Cyber and Jihad Lab*, November 4, 2014. Accessed May 5, 2015. http://cjlab.memri.org/lab-projects/tracking-jihadi-terrorist-use-of-social-media/isis-follower-on-twitter-warns-against-using-kik-messenger-service-when-chatting-about-sensitive-jihadi-stuff-recommends-other-technologies/

It's important to bear in mind, too, that even when citizens do not leave for the Syria-Iraq border presently controlled by ISIS, their support of extremist organizations threatens the security of the nation because terrorist objectives can be carried out within one's own borders. The attack in Paris just this past January at the offices of *Charlie Hedbo*, a satirical weekly magazine, in which 12 people were killed is clear evidence of the potential danger/

5. THE ATTRACTION TO ISIS

Husna Haq, a correspondent for *The Christian Science Monitor*, identified four (4) reasons why American teens, in particular, are lured into joining the terrorists of the Islamic State:[11]

First, these groups can provide youth with a sense of identity. "ISIS typically preys on Western youth who are disillusioned and have no sense of purpose or belonging."[12] This is similar to how urban gangs draw in disaffected, aimless youth, offering them a sense of family and purpose. "The general picture provided by foreign fighters...suggests camaraderie, good morale and purposeful activity, all mixed in with a sense of understated heroism, designed to attract their friends as well as to boost their own self-esteem."[13]

Secondly, ISIS operates a sophisticated propaganda machine.[14] Robert Hannigan, UK surveillance chief, stated that, "ISIS and other extremist groups use platforms like Twitter, Facebook and WhatsApp to reach their target audience in a language it understands. Their methods include exploiting popular hashtags to disseminate their message."[15] The group's use of social media allows for quick distribution of propaganda and invites a widespread following.

Yasir Qadhi, a Muslim cleric in the U.S. and professor at Rhodes College in Memphis, agrees that radicalization occurs not in mosques, but rather online, in secret. He relates that "...most parents are comfortable with a quieter Islam that tends to shy away from controversial matters, such as American policy in Muslim lands."[16] Consequently, there is a communication gap between the generations. And aside from the communication gap, the technology and social media sites that adolescents use daily can be confusing and unfamiliar to parents. There is an absence, Qadhi says, "...of genuine dialogue that could be tempered with some elderly wisdom."[17]

---

[11] Husna Haq, "ISIS Excels at Recruiting American Teens: Here Are Four Reasons Why," *The Christian Science Monitor*, October 22, 2014. Accessed April 25, 2015. http://www.csmonitor.com/USA/USA-Update/2014/1022/ISIS-excels-at-recruiting-American-teens-Here-are-four-reasons-why-video

[12] Ibid.

[13] Richard Barrett, Foreign Fighters in Syria [White paper], The Soufan Group, June 2014. Accessed April 25, 2015. http://soufangroup.com/foreign-fighters-in-syria/

[14] Haq, "ISIS Excels at Recruiting American Teens: Here Are Four Reasons Why."

[15] Jethro Mullen, J. (2015, Feb. 25). "What is ISIS' Appeal for Young People?" *CNN*, February 25, 2015. Accessed April 25, 2015. http://www.cnn.com/2015/02/25/middleeast/isis-kids-propaganda/

[16] Janet Reitman, "The Children of ISIS," *Rolling Stone*, March 25, 2015. Accessed April 25, 2015. http://www.rollingstone.com/culture/features/teenage-jihad-inside-the-world-of-american-kids-seduced-by-isis-20150325

[17] Ibid.

A sense of religious obligation, the third reason Haq gives for why American teens are lured by ISIS,[18] can often be a persuasive approach to convince young people to join the extremist group. The militants appeal to Muslims throughout the world to protect and defend fellow Muslims from attack.

> With the declaration of its "caliphate" in July 2014, ISIS began to enhance and amplify themes relating to the society it wanted to create, providing a new answer to the question: "Why join?" In his first speech as putative caliph, Abu Bakr al-Baghdadi reflected this new focus, calling on Muslims everywhere to make *hijra* "to the land of Islam" as a religious obligation.[19]

And fourth, Haq believes that ISIS' female-targeted recruitment draws in American adolescent girls.[20] This premise seems reasonable particularly for young female American-Muslims who may feel isolated and removed from their non-Muslim peers. Being brought up in a strict Muslim home, for girls, often means living with a number of restrictions. While these restrictions would still be compelled in the Islamic State— "ISIS women do not leave their homes without a mahram, a male family member who acts as their guardian, or without permission from their husbands, in which case they travel in groups"[21] —Western girls may anticipate a welcoming Muslim community offering companionship, likeminded friends their own age, and the fulfillment and gratification of feeling valued.

The blog entry, "Girl Talk" asserted the following:

> The increased social media recruitment efforts of women in the Islamic State to get higher numbers of women to move to Syria indicate an agenda beyond militaristic goals. As such female-run social media accounts describe a purposeful life in Syria while also providing information explaining how to enter the state, it is clear that women view themselves not only as educators of the Islamic State's youth, but also as crucial agents in adding to its population.[22]

Often the most effective ISIS recruiters of women are women. Umm Ubaydah is one such recruiter. Ubaydah, who herself left Europe for Syria early in 2014, posts a blog that encourages other women to make hijra, or migrate, to join the Islamic State. The posts include information about what to bring, how to dress, how much money will be required (which is linked to how long one plans to stay in Turkey), and what to expect once there—what daily life is like in Syria for women who make hijra. Other posts offer support, relating the difficulty, yet necessity, of leaving one's family. Erin Marie Saltman, a Senior Counter Extremism Researcher for the Institute for Strategic Dialogue (ISD), affirmed that women are quite successful as recruiters of other women because "there's a level of comfort established when conversing with another woman. Communicating with a woman can ease a

[18] Haq, "ISIS Excels at Recruiting American Teens: Here Are Four Reasons Why."

[19] J. M. Berger and Jessica Stern. "Why Are Foreign Fighters Joining ISIS?" *Defense One*, March 8, 2015. Accessed April 25, 2015. http://www.defenseone.com/threats/2015/03/why-are-foreign-fighters-joining-isis/106962/

[20] Haq, "ISIS Excels at Recruiting American Teens: Here Are Four Reasons Why."

[21] Reitman, "The Children of ISIS."

[22] "Girl Talk: Calling Western Women to Syria," [INSITE Blog on Terrorism and Extremism]. Accessed May 1, 2015. http://news.siteintelgroup.com/blog/index.php/about-us/21-jihad/4406-girl-talk-calling-western-women-to-syria

potential recruit's apprehension about leaving her family.[23] According to a CNN report, TRAC—the Terrorism Research and Analysis Consortium, estimates that nearly 1 in 6 ISIS foreign recruits are women.[24]

6. THOSE WHO FALL PREY

6.1 GREAT BRITAIN

The details of the case of three schoolgirls in London illustrate the power of social media to induce vulnerable young people to join ISIS. In February of this year, Amira Abase, just 15 years old, and her friends, Kadiza Sultana, 16, and Shamima Begum, 15, took a bus to Gatwick Airport and boarded a flight to Istanbul. From there they took a bus to Turkey's border with Syria where they were met by ISIS operatives who took the girls by car into Syria.[25]

The three girls were students at Bethnal Green Academy in East London. After a fellow classmate from the Academy left in December 2014 for Syria, police spoke to the three girls, "but concluded they were not being groomed by ISIS."[26] The school, Bethnal Green Academy, was reportedly criticized at first for seemingly supporting an environment where radicalization of youngsters could take hold. The Academy defended itself, however, pointing at social media as the medium for radicalization and maintaining that the Academy had instituted safeguards by disallowing students to access either Facebook or Twitter from the school's computers.[27] The Academy's position is further supported by accounts of Amira Abase's life leading up to her departure. One friend reported that as early as age 11, Amira had a smartphone and later a computer and that "she was on them all the time."[28]

Investigators believe that Shamima, one of the three London schoolgirls, connected online via Twitter with Aqsa Mahmood. In November 2013, Aqsa Mahmood (now known as Umm Layth) left her own moderate Muslim family and their affluent home in Glasgow, Scotland, and made her way to Syria. She was 19 years old at the time. Mahmood's family believes that Asqa was also likely radicalized online, making contacts online with others who persuaded her to join the extremists in Syria.[29]

---

[23] Katie Zavadski, "Meet the Female Recruiters of ISIS," *Daily Intelligencer*, September 4, 2014. Accessed April 11, 2015. http://nymag.com/daily/intelligencer/2014/09/meet-the-female-recruiters-of-isis.html

[24] "ISIS Lures Teenagers to Join Fight" [Video file], *CNN*, February 20, 2015. Accessed April 12, 2015. http://www.cnn.com/videos/world/2015/02/20/tsr-dnt-sciutto-isis-girls-to-syria.cnn

[25] Sue Reid, "From Joker to Jihadi Bride: Exclusive Pictures of the London Schoolgirl Who Ran Off to Join ISIS," *Daily Mail*, Last updated March 4, 2015. Accessed April 11, 2015. http://www.dailymail.co.uk/news/article-[illegible] year-old-s-run-join-ISIS.html

[26] Ibid.

[27] Holly Yan and Nima Elbagir, "Authorities Scramble to Find Teen Girls Before They Join ISIS" [Video file], *CNN*, February 23, 2015. Accessed April 12, 2015. http://www.cnn.com/2015/02/23/europe/uk-syria-missing-girls/index.html?sr=tw022315isismissinggirls830aVODtopPhotos

[28] Reid, "From Joker to Jihadi Bride."

[29] Pamela Engel, "This Scottish Teenager Went from Reading Harry Potter to Recruiting for ISIS in Syria," *Business Insider*, February 26, 2015. Accessed April 12, 2015. http://www.businessinsider.com/how-aqsa-mahmood-ended-up-recruiting-for-isis-in-syria-2015-2

6.2 AUSTRALIA

In Australia, too, supporters of the Islamic State connect via social media with ISIS operatives and other likeminded advocates of the extremist group. Users calling themselves "al-Australi" or "al-Astrali" (meaning "from Australia")—a surname often adopted by those who are connecting with the terrorist group from within Australia in order to hide their identity—are rampant on Facebook. "Strangers from all over the world are now meeting...to fight for a caliphate—a monotheistic Sharia Law state that they hope has its beginnings in Iraq and Syria, and will then overrun the world."[30]

In Australia, fears are heightened that teens in particular are being targeted by ISIS especially after, barely a month ago, two brothers—one aged 16, the other 17—were apprehended at the airport in Sydney. The pair were attempting to board a flight to the Middle East with the intent of ultimately fighting alongside ISIS militants. Items in their luggage included "extremist paraphernalia" as well as instructions for formulating a story to avoid suspicion from authorities as they left the country.[31] The fact that the two brothers were so young and that they were native Australians stunned many. "The boys had become radicalised jihadists over the Internet and officials said their parents were 'as shocked as any of us would be' when they were told their children planned to join the violent terrorist group."[32]

Although Australian law enforcement has reportedly revoked 100 passports due to security concerns related to the specific individuals, recent reports indicate about 100 Australians have left the country to join the Islamic State militants. "The latest figures come as an Australian ISIS fighter in Syria resurfaced on Twitter to mentor prospective jihadists on how to join the death cult."[33] Connecting with potential recruits via social media, "mentoring" involves linking young Westerners who support ISIS to the financial means to travel to the Middle East and providing them with contacts in Turkey—a key point of entry into Syria for foreign fighters.

6.3 UNITED STATES

Young people in the United States are not beyond the reach of ISIS either. In January 2015, a 19-year old American girl from Colorado, Shannon Maureen Conley, was sentenced to four years in prison for conspiracy to provide material support to a designated foreign terrorist organization. According to her family, Shannon had learned everything she knew about Islam from the Internet. While her family was aware that Shannon had converted to Islam, they were taken completely by surprise when they learned she was involved with jihadists. Conley's father had found an air ticket for his daughter to fly to Turkey and contacted authorities. Conley was arrested in April 2014 at

---

[30] "Facebook Riddled with Australian Muslims Supporting ISIS," *www.news.com.au*, August 24, 2014. Accessed April 21, 2015. http://www.news.com.au/technology/online/facebook-riddled-with-australian-muslims-supporting-isis/story-fnjwmwrh-1227034437804

[31] Jane Onyanga-Omara, "Teens Stopped at Sydney Airport on Suspicion of Trying to Join ISIL," *USA Today*, March 8, 2015. Accessed April 21, 2015. http://www.usatoday.com/story/news/world/2015/03/08/teens-stopped-islamic-state/24601625/

[32] Lucy Clarke-Billings, "ISIS Targets Australian Teenagers to Join 'Death Cult' Amid Fears They Will Be Used as Cannon Fodder." *The Independent*, March 9, 2015. Accessed April 21, 2015. http://www.independent.co.uk/news/world/middle-east/isis-targets-australian-teenagers-to-join-death-cult-amid-fears-they-will-be-used-as-cannon-fodder-10095342.html

[33] "More Australians Joining ISIS with 30 Deaths Confirmed," *www.news.com.au*, April 18, 2015. Accessed April 21, 2015. http://www.news.com.au/national/more-australians-joining-isis-with-30-deaths-confirmed/story-fncynjr2-1227308688607

Denver International Airport where she was attempting to board a flight to Frankfort, Germany; she had planned to fly to Turkey from there. Conley apparently told authorities she was meeting a suitor she'd met on the Internet, a 32-year old Tunisian man who was an ISIS soldier. Conley, a certified nurse's aide, expressed her intent to marry this man and "become a nurse in an ISIS camp."[34] During their investigation, agents uncovered al-Qaeda materials and DVDs of Anwar al-Aulaqi (an American-born Islamic cleric who was involved with al-Qaeda and a number of terrorist attacks) in Conley's home. At her sentencing, Conley insisted she understood now that the extremist views of those she'd planned to unite with abroad were twisted interpretations of the Quran. However, statements that Conley allegedly made even while she was in jail awaiting trial demonstrated continued support of violence and jihad.

Recently, *Rolling Stone* magazine featured a story about three teenagers from the same suburban-Chicago Muslim family who were detained at O'Hare International Airport early in October, 2014. Authorities did not disclose how their suspicions were raised about these three siblings, but authorities were on the lookout that day, specifically looking for the three at the airport. The oldest of the three, Hamzah Khan, aged 19, was arrested for "...'knowingly attempting to provide material support and resources' to a foreign terrorist organization in the form of personnel — namely, himself."[35] Because Hamzah's siblings were younger—his sister was 17 and his brother just 16—they have not yet been charged with a crime, but it's likely in time they will be.

The story of these Midwestern suburban teenagers highlights the difficulties of growing up Muslim in the United States, particularly in this post-9/11 era. Many Muslims in the U.S. feel that they have lived under a constant veil of fear and suspicion. Many feel they have been unfairly harassed, having been pulled aside at the airport by TSA as they traveled, or at the very least, being on the receiving end of nervous, distrustful stares. "Many Muslim families [know] of at least one child who'd been teased and called 'Osama' or 'terrorist' on the playground."[36] Furthermore, for the whole of these teenagers' lives, the United States has been involved in wars in predominantly Muslim countries—Afghanistan and Iraq. American-Muslims often feel as though they don't belong—a dangerous state of mind for impressionable young people who are looking to fit in.

Growing up, the three Khan children did not attend their local suburban public school. They were instead educated at an Islamic primary school and, when they were older, an Islamic day school. At age 10, Hamzah left school for more than two years to become a hafiz. (A hafiz is someone who has memorized the Quran.) "It's not uncommon in highly religious Muslim families, particularly those from the South Asian community, to put their kids through this program, which is both a sign of piety and great prestige."[37] Hamzah's sister also became a hafiz and was home-schooled during the three year process; these were her middle school years. After completing the hafiz program, Hamzah's sister did not feel comfortable returning to school and attending, at that point, high school. Instead she continued her studies through a correspondence program. According to Ahmed Rehab, executive director of the Chicago branch of the Council on American Islamic Relations, this type of upbringing [illegible] with the risk of setting them up for profound isolation."[38]

---

[34] Michael Martinez, Ana Cabrera and Sara Weisfeldt, "Colorado Woman Gets 4 Years for Wanting to Join ISIS," *CNN*, January 24, 2015. Accessed April 25, 2015. http://www.cnn.com/2015/01/23/us/colorado-woman-isis-sentencing/

[35] Reitman, "The Children of ISIS."

[36] Ibid.

[37] Ibid.

[38] Ibid.

It's apparent that American culture does not always align with Muslim norms and values. Particularly for young women, the style of dress that is expected in traditional Muslim families is far more modest. Dating in a conventional American sense—a teenage boy and girl going out together on their own to a movie, for instance—would not be permitted in a family that strictly adheres to Islamic laws and customs. The dichotomy that exists between the American and Muslim cultures can cause Muslim teenagers in the United States to feel isolated and disconnected from their peers.

On the reverse, though, adolescents living in Western cultures have virtually *no* restrictions as to whom they connect and interact with when communicating over the Internet—and this is true for both Muslim and non-Muslim teens alike. Parents often have little, if any, knowledge of the contacts and associations their teens are making privately from their own computers and smartphones. For teenage girls raised in strict Muslim households who may perhaps live decidedly sheltered lives, behavior that would be prohibited in their daily lives—communicating one-on-one with a young man without another male family member accompanying, for example—is completely feasible when the interaction occurs over the Internet.

7. CONCLUSION

The grooming process used by ISIS in recruiting teenage girls over the Internet is analogous to the tactics used by online predators. A pedophile gains the trust of the victim over time and persuades the victim to keep the relationship secret. "When the time is right he convinces the child to leave her family and join him. The process is identical in radicalization by ISIS."[39] With the rising number of young people being lured into joining the extremists, Anwar argues that the problem should be regarded as a child protection issue.[40]

This approach seems quite reasonable. For the most part, officials have not disclosed how they've come to identify many of the would-be ISIS recruits—stopping them at airports as they're attempting to leave the country. It's probable, though, that authorities are tracking communications between ISIS and the foreigners who are "following" them, and perhaps even more likely, posing as ISIS members or ISIS supporters in order to draw in followers. This "impersonation" tactic is similar to the *Dateline NBC* feature, "To Catch A Predator," in which child sex predators were rooted out on the Internet by authorities who—in online chat rooms—pretended to be underage girls or boys who had agreed to meet adults (the suspected predators) for sex.

It's a losing battle to shut down every Twitter account operated by suspected terrorists, delete their Facebook accounts, or take down YouTube videos posted by ISIS—unless the content specifically violates the Terms of Service for those sites. Reis likened the prospect to a game of "Whac-a-Mole"—as soon as one account is shut down, there's another popping up.[41] Not to mention that freedom of [illegible] Twitter or Facebook accounts willy-nilly because we disagree with others' views is completely contrary to this ideology.

The better option is to use the social media platforms ISIS uses to advance our own objectives—to track the terrorist group and its operatives and to identify the at-risk populations ISIS attempts to connect with. In addition, following ISIS on social media allows the U.S. and other Western nations to understand the reasons that young citizens are drawn to extremist groups, as well as to learn how to better combat ISIS recruitment efforts—whether the purpose of recruitment is to induce prospective "foreign fighters" to travel overseas or to persuade sympathizers to carry out terrorist attacks inside the borders of their own countries.

---

[39] Aamer Anwar, "How ISIS's $2B Budget Helps It Recruit Western Teenagers to Terrorism," *CNN*, March 27, 2015. Accessed April 21, 2015. http://www.cnn.com/2015/03/27/opinions/aamer-isis-recruiting-western-teenagers/

[40] Ibid.

[41] Reis, "Twitter's Terrorist Policy."

HORIZON 2020

Media Warfare and the Discourse of Islamic Revival: The Case of the Islamic State (IS)

Reporting

Project Information

MWDIR

Grant agreement ID: 707482

DOI
10.3030/707482

Closed project

Start date
1 February 2017

End date
31 January 2019

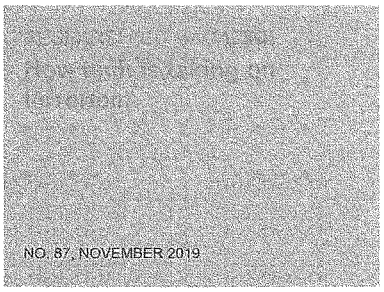
Funded under
H2020-EU.1.3.
H2020-EU.1.3.2.

Overall budget
€ 195 454,80

EU contribution
€ 195 454,80

Coordinated by
UNIVERSITY OF NEWCASTLE UPON TYNE
United Kingdom

This project is featured in...



Periodic Reporting for period 1 - MWDIR (Media Warfare and the Discourse of Islamic Revival: The Case of the Islamic State (IS))

Reporting period: 2017-02-01 to 2019-01-31

Summary of the context and overall objectives of the project

Broadly speaking, the developments and changes in dynamic of communication have challenged traditional notions in mass media scholarship e.g. media power, representation and audiences (KhosraviNik , 2014). A trajectory of such 'notional' change has affected norms of political communication in general and political activism in particular. 'Ordinary' users become part of production, consumption and distribution of content with few or no barriers in the form of traditional gate-keeping practices (Unger, Wodak, and KhosraviNik , 2015).

In such environment, radical movements exploit social media to mobilise new recruits by reinforcing certain discourses. In other words, IS employs strategic rhetorical propaganda by which it attracts not only (young) individuals from the Middle East, but also from EU countries, the United States of America and other regions. Increasingly, the radical and fundamentalist thrust of IS seems to be at odds with other Islamist movements, e.g. Hamas, the Muslim Brotherhood and even Al-Qaeda. The thorough review of the literature on these movements indicates that there are two overlapping discourses which dialectically feed into each other to form the essence of the IS worldview, namely the discourses of religious revival and political emancipation. The former is a manifestation of a universal propensity in all religions, faced with a perceived threat of modernity to their traditional established worldview. The latter is a political and ideological framework. This project claims that the rise and "success" of IS discourse is to be examined within a wider socio-political contextualisation of matters of identity, migration, multiculturalism, etc. As such, the current project has investigated the IS propaganda model based on Critical Discourse Analysis.

In examining the discourse of the Islamic State (IS), this study has aimed to answer the broad question: 1) How does IS construct itself in propagating its discourse worldwide? In answering this general question, the study aimed to answer these sub-research questions

1. What rhetorical propaganda devices are manifested in IS discourse?
2. What are the visual frames employed in IS' self-constructions?
3. What conclusions can be drawn from analysis of IS discourse?

This project is important for the society in two dimensions:
1) This project contributes to understanding of IS's ideological discourse and its impact and consequences for the EU. Without understanding the socio-political and cultural –religious dimensions and the ensemble of discourses that frame them, Islamic fundamentalism in general, and IS' in particular, are liable to be discounted as merely fringe movements with an apocalyptic agenda. This project expounds security consequences for the EU that might rise from IS mobilization of people.
2) This project has contributed to the study of discourse of Islamist movements during times of crises or conflicts and on how this discourse has a high-impact on influential mechanisms that affect societies.

The overall objectives of the project were
1. To map the general politics of ethnicity, language and culture in the context of Islamist movements.
2. To examine language representation, i.e. the specific perspectives from which Islamist movements are constructed and the language used in their texts or talks to assign meanings to them and their social practices.
3. To critically examine the power relations between the discourse of Islamist movements and their self-representation.

Work performed from the beginning of the project to the end of the period covered by the report and main results achieved so far

The researcher has performed several actions inside and outside the host university in collaboration with and under supervision and guidance of the supervisor. In this report, I divide the actions into academic/scientific, publicity/engagement and training.
1. Academic actions:
-Reviewing Literature and Setting up the Methodological Approach.
-Pilot Study and Data Analysis.

In doing these actions, several deliverables have been done:
- Submitting a research report on studies on IS in multi-disciplinary studies to my supervisor.
- Submitting a report to the supervisor on the data collected from social media (YouTube).
- Organising several meetings with PhD students at Newcastle University. Those students worked on IS and war reporting. These meetings discussed challenges and applicability of CDA in Social Media and in media studies.
- Writing a journal paper on challenges in data collection and analysis in social media.
- Organising a training session with PhD and MA students on how to collect data from YouTube.

2. Publicity/engagement with public

To publicise the results of the analysis, I have highly engaged with various audiences in different places, institutes and countries. This strategy included participation in meetings, conferences and workshops. The aim was to raise awareness of IS' propaganda, discourse, philosophy and politics. The publicity and engagement with public has been conducted throughout the whole period of the project.

Teaching and Presentation for students. I have engaged in teaching some lectures as a guest lecturer at Media, Culture and Heritage department.
Visiting Research. I have also been engaged with research groups outside Newcastle University.

Workshops and meetings and engagement with Marie Curie. Also, I have been engaged with Marie Curie Alumni Association and Marie Curie Actions Association.

For public community, I have organized a guest lecture at the Oriental and African Studies Institute at Hamburg University (Germany).

I have been trained in several dimensions at Newcastle University: computer software to analyse data, Collect Data from social media platforms

Progress beyond the state of the art and expected potential impact (including the socio-economic impact and the wider societal implications of the project so far)

"The analysis of the data has shown that IS uses every possible means in exploiting social media to mobilise and recruit people. The so-called ""Islamic State"" has enthusiastically embraced and capitalised on new communicative affordances of the participatory web. Obviously, the rise and "success" of IS discourse needs to be examined towards the analysis of IS's social media practices within a wider socio-political contextualisation of matters of identity, migration, multiculturalism, etc. In applying SM-CDS, the analysis comes up with major findings in regard to IS's social media practices and tactics. These findings can be summarised as follows:

A) Share, Distribution and Dissemination of IS's publications online, e.g. videos, photos, texts, ...etc.
A) Create fake or anonymous accounts on social media platforms
B) Make and publish videos and films of high quality

In exploring IS's visual frames and legitimation, IS builds its legitimations on several strategies in analysing IS videos on burning the Jordanian pilot:
• IS's indictment against the Jordanian Regime of Betrayal and Espionage
• The pilot's participation in the military airstrikes on the IS-controlled areas

- The king of Jordan is represented as apostate.
- The king Abdullah is accused of sending pilots to fight against the Islamic State's jihadist
- Facing a military judgement with evidences

In consideration of current initial results and the challenges facing researching social media and terrorism, we can highlight the following implications

1. Highlighting Security Threats at Local and International Levels: more terrorism and violent actions
2. Building and Networking: and Creating Online Radical Community

"

publications-march-2019-1.jpg

Last update: 26 June 2019
Record number: 382560

Permalink: https://cordis.europa.eu/project/id/707482/reporting

HORIZON 2020

Media Warfare and the Discourse of Islamic Revival: The Case of the Islamic State (IS)

Fact Sheet

Project Information

MWDIR

Grant agreement ID: 707482

DOI
10.3030/707482

Closed project

Start date
1 February 2017

End date
31 January 2019

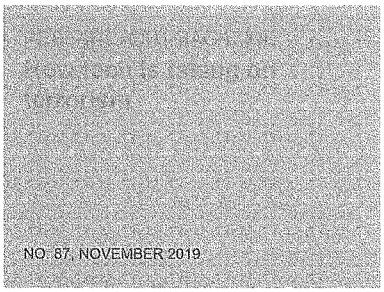
Funded under
EXCELLENT SCIENCE - Marie Skłodowska-Curie Actions

Total cost
€ 195 454,80

EU contribution
€ 195 454,80

Coordinated by
UNIVERSITY OF NEWCASTLE UPON TYNE
United Kingdom

This project is featured in...



Objective

This proposal seeks to better our understanding of how Islamist movements use Social Media to reinforce their discourses, ideologies and thoughts during times of conflict, i.e. ideological levels of struggle. In brief, this study takes as its mission the task of unravelling patterns of rhetorical propaganda employed by the Islamic State (IS) and how this movement attracts individuals from all over the world and influences security in Europe and the world. There are two overlapping discourses which dialectically feed into each other: those of religious revival and political emancipation. By means of these discourses, IS reworks foundational myths and traditional religious symbols to appropriate an imagined past in a highly charged political and conflict-ridden context as a part of the solution to its beleaguered spirituality.

This proposal suggests employing interdisciplinary methods: critical discourse analysis (CDA), Corpus Linguistics, visual content analysis and multi-modal analysis. This aims to examine discourse, content and visual frames. The sample is supposed to include all YouTube video clips published by IS and the commentaries associated with these clips in English and Arabic.

The importance of this project lies in understanding the socio-political and cultural-religious dimensions of the conflict and the ensemble of discourses that frame Islamic fundamentalism in general, and IS in particular, as well as how IS persuades recruits from the EU and worldwide. This project is significant in opening a new academic career path for me and in giving me an opportunity to apply for professorship/senior lecturer and chair positions in media and communication, sociolinguistics and discourse of Islamist movements in future.

Fields of science

social sciences › political sciences › **political communication**

humanities > languages and literature > **linguistics**
natural sciences > computer and information sciences > **software**
humanities > philosophy, ethics and religion > **religions**
humanities > philosophy, ethics and religion > **philosophy**

Programme(s)

H2020-EU.1.3. - EXCELLENT SCIENCE - Marie Skłodowska-Curie Actions (MAIN PROGRAMME)

H2020-EU.1.3.2. - Nurturing excellence by means of cross-border and cross-sector mobility

Topic(s)

MSCA-IF-2015-EF - Marie Skłodowska-Curie Individual Fellowships (IF-EF)

Call for proposal

H2020-MSCA-IF-2015

See other projects for this call

Funding Scheme

MSCA-IF-EF-ST - Standard EF

Coordinator

UNIVERSITY OF NEWCASTLE UPON TYNE

Net EU contribution

€ 195 454,80

Address

Kings Gate
NE1 7RU Newcastle Upon Tyne
United Kingdom

Region

North East (England) > Northumberland and Tyne and Wear > Tyneside

Activity type

Higher or Secondary Education Establishments

Links

Contact the organisation Website
Participation in EU R&I programmes
HORIZON collaboration network

Other funding

€ 0,00

EC signature date: 24 February 2016
Last update: 12 August 2022
Record number: 204939

Permalink: https://cordis.europa.eu/project/id/707482

European Commission

HORIZON 2020

Media Warfare and the Discourse of Islamic Revival: The Case of the Islamic State (IS)

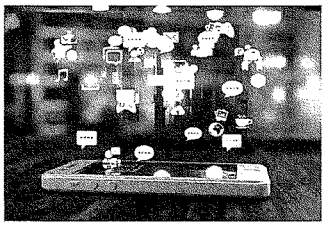
Results in Brief

DE EN ES FR IT PL

A critical discourse approach offers insights into terrorist movements' social media use

Social media have provided many social, religious and political movements an effective means for networking and communicating with diverse stakeholders. EU researchers examined Islamic State's (IS) own use of online platforms to reinforce its ideologies.

SOCIETY



© Lenka Horavova, Shutterstock

MWDIR project coordinator Dr Majid KhosraviNik makes the introduction: "IS has enthusiastically embraced and capitalised on new communicative affordances of the participatory web." Dr KhosraviNik and the project's Marie

Curie research fellow Dr Wesam Amer delved into the social media practices of IS's members, followers and supporters. This involved examining online communicative practices and patterns of rhetorical propaganda (overlapping discourses).

Communication analysis from a sociological perspective

MWDIR employed social media critical discourse studies (SM-CDS). "CDS offers interpretations and explanations of the meaning-making processes by situating the content materials in both the digital media and social contexts in which they occur," Dr KhosraviNik explains. His published book chapter 'Social media critical discourse studies' elaborates on the approach, which offers a sociological take on communication analysis. He notes: "By employing SM-CDS, the project has identified patterns of similarities and differences in the way IS constructs itself, its purported enemies as well as digital practices employed for propaganda and recruitment."

Data analysis revealed and explained why IS's communicative strategies appear to resonate with an important portion of Muslim youth both in Europe and worldwide. "Examination of discursive practices showed how the discursive politics of self-representation and identity in general play a role in such a movement," the coordinator reports. The research also analysed visual media content, utilising a visual framing model to examine visualisation and other modalities of discourse.

The fundamentals of IS strategy

MWDIR researchers present the ensemble of discourses that frame Islamic fundamentalism in two points. The first covers IS's reworkings of foundational myths of traditional religious symbols to appropriate an imagined past community in a politically charged and conflict-ridden context.

The second point refers to the strategic rhetorical propaganda IS employs to attract individuals from the EU, Middle East and the United States, and many other regions. "IS's discourse pivots around combating the constructed/perceived threat to its most sacred values in the context of a confrontation with an 'other' in a process one could call 'mimetic violence'," Dr KhosraviNik sums up.

Contributions and accomplishments

MWDIR outcomes contribute to our understanding of how IS constructs itself on the socio-political and cultural-religious dimensions of conflict with the

'other'. Against this background, Dr KhosraviNik and Dr Amer underline the need to consider the context of use and circularity of data. It is not coming from just one concentrated source, and there is no clear notion of what is and what can be considered IS materials, or what is coming from sympathisers or what constitutes a harmless religious opinion.

Project accomplishments go beyond topic-specific research. "This project has contributed to ongoing debate on how to do CDS in social media research within a contextual approach to meaning-making," Dr KhosraviNik expresses. It also provided the researcher with advanced analytical skills as well as competences in applying CDS in social media discourse as an emerging and essential field.

"The project contributes to European excellence and European competitiveness by diminishing the fragmentation of terrorism in social media studies from linguistic, media and security dimensions," he concludes. MWDIR brings forward new ideas and represents an important step forward in scientific knowledge regarding the social media practices of terrorist movements.

Keywords

MWDIR, IS, social media, critical discourse studies, SM-CDS, terrorist movement, communication analysis, Islamic State, participatory web

Project Information

MWDIR

Grant agreement ID: 707482

DOI
10.3030/707482

Closed project

Start date
1 February 2017

End date
31 January 2019

Funded under
H2020-EU.1.3.
H2020-EU.1.3.2.

Overall budget
€ 195 454,80

EU contribution
€ 195 454,80

Coordinated by
UNIVERSITY OF NEWCASTLE UPON TYNE
United Kingdom

This project is featured in...

Discover other articles in the same domain of application

Inequalities as barriers to inclusive long-term care

8 September 2020

RESULTS IN BRIEF

SCIENTIFIC ADVANCES

Supporting resilience in rural communities to face life-changing challenges

29 November 2019

NEWS

SCIENTIFIC ADVANCES

Size matters: Small city people more likely to migrate than large city ones

20 September 2018

NEWS

Last update: 5 August 2019
Record number: 397830

Permalink: https://cordis.europa.eu/article/id/397830-a-critical-discourse-approach-offers-insights-into-terrorist-movements-social-media-use

WORLD

A new group of TikTok-savvy Palestinian fighters tests Israeli forces in the West Bank

Updated October 26, 2022 · 2:52 PM ET

DANIEL ESTRIN

3-Minute Listen PLAYLIST Download

Mourners attend the funeral of Palestinians killed in an overnight Israeli raid in the occupied West Bank city of Nablus on Tuesday. The Israeli army said it was targeting an emerging armed group called Lions' Den.

Jaafar Ashtiyeh/AFP via Getty Images

TEL AVIV — This year has already been the deadliest Palestinians have experienced in the Israeli-occupied West Bank in many years. But a brazen Israeli special forces operation before dawn Tuesday, which killed five Palestinians, including at least one militant, and wounded 20, was this year's single bloodiest confrontation in the West Bank yet.

Israel's target was not one of its usual suspects, like the Hamas or Islamic Jihad militant groups. It was the Lions' Den, a new renegade group of young armed men, many in their teens and early 20s. They are small in number — analysts estimate between 50 to 100 — but big in influence.

Lions' Den militants have shot at Israeli troops and checkpoints, and sought refuge in the narrow alleyways of the old casbah in the West Bank city of Nablus. The Israeli army says the group has shot dead at least one of its soldiers.

Prime Minister Yair Lapid said Tuesday on Israel Army Radio that much of the country's forces are now focused on their pursuit. "This was a lethal precision strike at the heart of a terrorist cell that was trying to carry out attacks," Lapid said in a statement about Tuesday's raid, in which the Israeli army killed a 31-year-old Lions' Den leader, Wadee al-Huh.

The Israeli army used shoulder-launched missiles during the raid and claimed to have blown up what it said was a bomb lab.

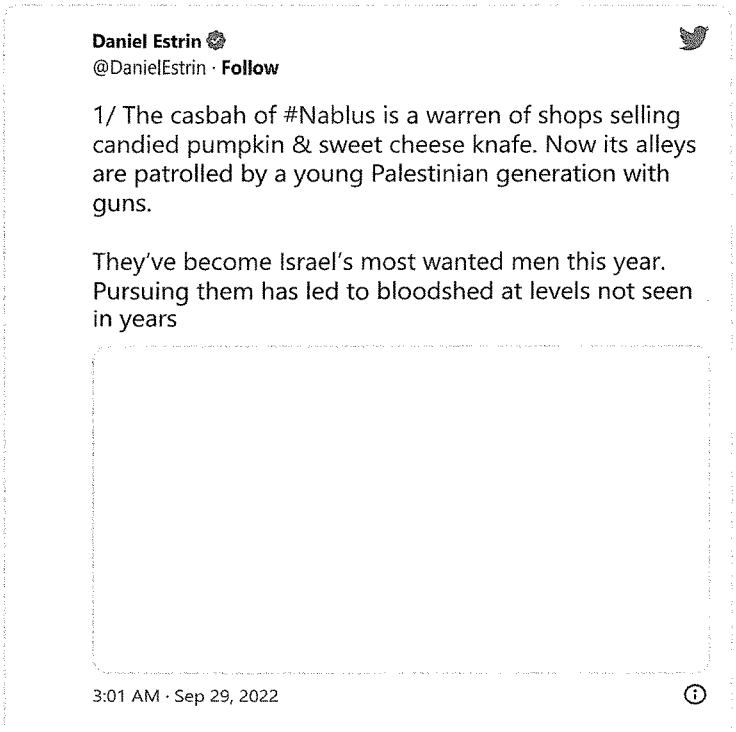
Israeli troops continued their operations, saying they arrested three suspected Lions' Den operatives in Nablus early Wednesday.

The escalating violence comes less than a week before the Israeli elections on Nov. 1.

Here is a brief look at the Lions' Den, and how it offers a glimpse into what the future could bring for the West Bank.

A young generation feels it has little to lose

Palestinian analysts and local community leaders in Nablus describe the group as a new generation of Palestinians who feel they have little to lose.



They don't have personal memories of the costly intifada of the early 2000s that migh caution them against violence. They grew up after Israel erected its wall-and-fence barrier and tightened its entry permit regime, so some of their only interactions with Israelis are with occupation-enforcing soldiers or often hostile settlers. They have

come of age under an ossified Palestinian leadership that blocks elections and offers no clear path forward to independence, analysts say.

"There's a lack of trust in any political horizon and in the Palestinian Authority. That's led the Palestinian youth to launch their own initiative and their own struggle against the Israeli occupation. And they've taken authority into their own hands," Jamal Tirawi, a prominent activist in Nablus and critic of the Palestinian leadership, tells NPR.

The group's aim is to confront Israeli soldiers when they operate in Palestinian areas – and to present an alternative to the behavior of the official Palestinian security forces, which do not clash with Israeli troops conducting arrest raids.

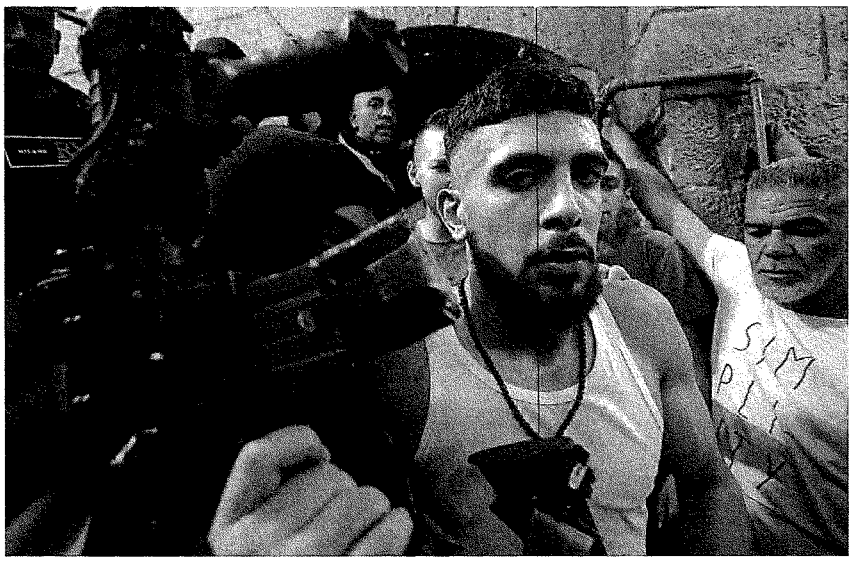
They amassed a massive TikTok following

MIDDLE EAST

A new generation is posing a challenge in the Israeli-occupied West Bank

The Lions' Den emerged earlier this year when Israel launched near-nightly military raids to pursue Palestinian militants amid a wave of deadly attacks on Israelis. Instead of the usual response by Palestinian youth — throwing stones and improvised explosives — these young men started opening fire at troops instead, often using M-16s smuggled from Israeli army supplies, according to the Israeli military.

The first Lions' Den militant to rise to prominence was Ibrahim al-Nabulsi, 18. He evaded several Israeli arrest attempts, then walked openly through the streets of Nablus, as crowds followed him and filmed him on the social media app TikTok. Israeli special forces killed him in Nablus' casbah in August. Now young Palestinians in Nablus wear necklaces bearing his portrait.



Ibrahim al-Nabulsi in Nablus on July 24.
AFP via Getty Images

Recently, when the Lions' Den made calls on social media for Palestinians to go out to the streets at a certain hour and shout "God is greatest!" — the calls were widely heeded. For the TikTok generation, admiration for the group is viral.

Israel says pursuing the Lions' Den sparks a "cycle of violence"

Israel's Shin Bet internal security chief Ronen Bar, in a recent speech, acknowledged the "cycle of violence." He said Israeli troops go after militants because the Palestinian

Authority's forces refuse to, which leads to firefights and more Palestinian casualties, further undermining the Palestinian security forces and leadership.

There have been attempts by the United Nations to call for calm. The Palestinian Authority mayor of Nablus recently met with Lions' Den members, urging them to consider an amnesty deal with Israel if they turned themselves and their weapons in to the Palestinian security forces. The militants reportedly rejected the offer.

These dynamics reflect a vacuum of leadership in the West Bank, and glimpses of what may come.

The old guard — the Palestinian Authority and their police forces — is losing credibility, and also losing control over pockets of the West Bank like the old city of Nablus. The young militants, meanwhile, are becoming more assertive. Israel is pursuing more targeted attacks against militants, even partially blockading Nablus recently in an attempt to confine them.

"The terrorists acting against us in [the West Bank] need to know there are two alternatives: either prison or the grave. They'll end up in one of the two," Defense Minister Benny Gantz told Israeli Channel 12 TV on Tuesday.

Though Israel is determined to stamp out the Lions' Den, the real significance of the armed group is not its numbers, but the inspiration it sparks in Palestinians throughout the West Bank.

Finally, Palestinians under occupation say, they have heroes they can rally around.

Opinion

Taking a TikTok journey straight to the Lions' Den

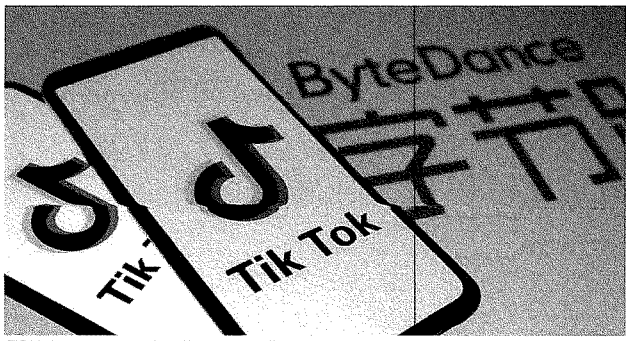
I tell this story not as a warning of the dangers of TikTok or social media, nor to promote content moderation on these platforms. Rather, I tell this story as a warning about the type of world we now live in.

Eitan Goldstein 10:33, 31.10.22

TAGS: TikTok Social Media Online Lions Den Opinion

Earlier this week I was speaking to a friend of mine about the rise of the Lions' Den terror cell in the city of Nablus in the West Bank. We were talking about how their rise was largely a result of becoming TikTok famous, with terrorists posting TikToks of themselves shooting at Israeli civilians and soldiers. As someone who speaks Arabic and follows various Palestinian channels on Twitter to understand their media landscape and how they view the world, I was intrigued as to how videos on TikTok, an app I had yet to download, were influencing this new generation of Palestinians.

I remarked that it would be interesting to see how long it took for the TikTok algorithm to begin showing me these Lions' Den videos, to which my friend replied, "only a crazy person would do that."



TikTok is the most popular app in the world (Photo: Shutterstock)

A few minutes later, with TikTok downloaded, I began my search for the Lions' Den videos that were inspiring this new generation of Palestinian terror.

Some notes:

- I didn't sign up for TikTok using any email, phone number, or identification of any kind.
- I came into this with a basic knowledge of the TikTok algorithm – the faster you swipe over something the less likely you are to see something similar. Conversely, the longer you watch a video, or even repeat a video, the more likely the algorithm is to show you similar ones.

- I went into this racing to see how fast I could find the videos. This was not a natural progression, rather a concerted effort to find these Lions' Den videos.

7:00 PM: I turned on TikTok and it asked me for some subjects I would be interested in. My phone is set to Hebrew, so I picked "קומדיה" (comedy). And with that, I was off!

For the first few minutes, I was getting a lot of Hebrew standup comedians and skits which I quickly scrolled past. Finally, I found one in Arabic and watched the whole thing twice. I then started getting more Arabic comedy. In addition, there were videos of Latina girls twerking to reggaeton songs in barely-there bikinis.

7:11 PM: I now began getting a lot of Syrian Druze TikTok videos talking about the Syrian Druze town of Suwayda, Syrian Druze history, and more. While interesting, I was on a mission and kept swiping until I found people speaking in a Palestinian dialect. It was then that I stumbled upon an old woman singing a song about Palestine. Fantastic. I watched it twice. I then started getting more nationalist Palestinian material. In addition, there were videos of very attractive Arab and Latina girls dancing to Arabic pop songs girls wearing skimpy, tight-fitting outfits. No more girls in bikinis.

7:48 PM: TikTok is now showing me videos made by Palestinians in the West Bank. I'm starting to hear a West Bank Palestinian accent in the videos, seeing lots of weddings, luxury car racing, people riding (and falling off) horses, people building houses, and more. But they're coming from all over the West Bank. I'm getting close! I quickly scroll past videos from Ramallah, Bethlehem, and Jericho and fully watch videos from Nablus and Jenin, as these are the cities where Lions' Den is the strongest. There are still attractive girls dancing to Arabic pop songs, but they're all wearing tight-fitting shirts and pants. Much more conservative.

8:46 PM: It finally happened. I got the algorithm to show me my first somewhat militant video. It's a video of a man standing next to homemade tank traps in Jenin vowing to "crush the occupation." I'm getting closer! There are no more cute girls dancing.

8:53PM: I've finally done it. My first Lions' den video! And it took me a little under two hours of searching. I'm seeing them being cheered on by Palestinians, getting into shootouts with the IDF, shooting at civilian buses and cabs, and imams praising their work, and all with the same soundtrack. I wonder how deep the rabbit hole goes and continue on.

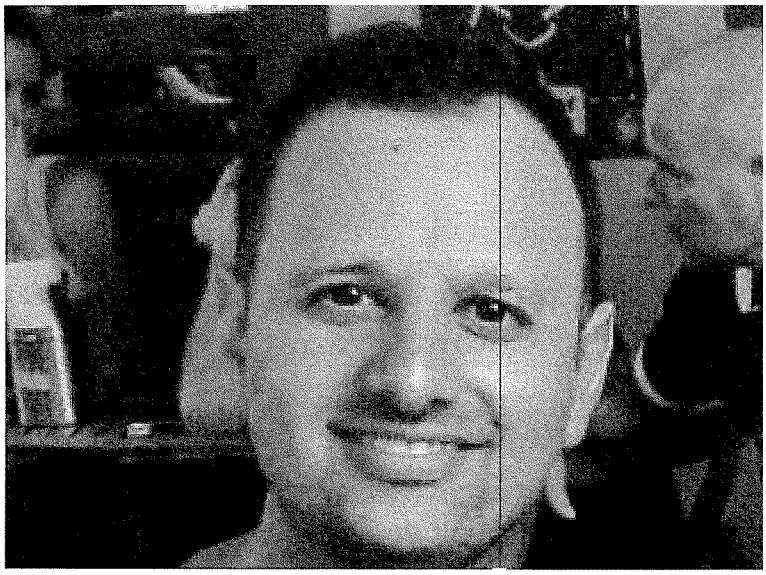
9:46PM: After watching about an hour of Lions' Den videos I'm shown one which is quite surprising – a video on how to make pipe bombs out of fire extinguishers and other household items. I'm then almost immediately shown part two with the terrorists placing the pipe bombs next to the Jalame checkpoint in the Northern West Bank outside of Jenin. And another one of a failed IED attack on an IDF convoy.

I tell this story not as a warning of the dangers of TikTok or social media, nor to promote content moderation on these platforms (a nearly impossible task). Rather, I tell this story as a warning about the type of world we now live in.

TikTok's algorithm is designed to give people exactly what they want so they'll stay on the app longer. Indeed, I felt a bit of excitement every time a new video popped up, and that dopamine hit felt like a drug. I was searching for something specific, and the algorithm did exactly what was asked of it - no more, no less.

I don't believe TikTok or any other social media app actively pushes extremism such as violence, sex, fake news, or unhealthy diets, just like it didn't push me to find these Lions' Den videos. Subconsciously, the human condition is predisposed to engage with more extreme videos, and the TikTok algorithm is designed to give users exactly what they want, whether or not they're cognizant of wanting it.

Therefore, I suggest something different – use the apps. However, be aware of what you're watching when using them, as it can quickly lead you down a path toward extremism. If you feel a video or post may lead the algorithm to suggest more extreme content, recognize it and swipe away quickly. I peered down the rabbit hole, and there's a long way to the bottom.



Eitan Goldstein(Photo: Eitan Goldstein)

Eitan Goldstein is the Communications Manager for a tech firm in Israel. He previously worked in law and as a senior editor for Ynetnews, Ynet's English Language news site. He holds a law degree from the College of Law and Business in Ramat Gan as well as a degree in International Relations from American University in Washington DC. Originally from Indianapolis, IN, Eitan lives in Tel Aviv, Israel.

TAGS TikTok Social Media Online Lions Den Opinion

START
NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM

RESEARCH BRIEF

The Use of Social Media by United States Extremists

SUMMARY

Emerging communication technologies, and social media platforms in particular, play an increasingly important role in the radicalization and mobilization processes of violent and non-violent extremists (Archetti, 2015; Cohen et al., 2014; Farwell, 2014; Klausen, 2015). However, the extent to which extremists utilize social media, and whether it influences terrorist outcomes, is still not well understood (Conway, 2017). This research brief expands the current knowledge base by leveraging newly collected data on the social media activities of 479 extremists in the PIRUS dataset who radicalized between 2005 and 2016.[1] This includes descriptive analyses of the frequency of social media usage among U.S. extremists, the types of social media platforms used, the differences in the rates of social media use by ideology and group membership, the purposes of social media use, and the impact of social media on foreign fighter travel and domestic terrorism plots.

The PIRUS data reveal four key findings on the relationship between social media and the radicalization of U.S. extremists:

- Online social media platforms are playing an increasingly important role in the radicalization processes of U.S. extremists. While U.S. extremists were slow to embrace social media, in recent years, the number of individuals relying on these user-to-user platforms for the dissemination of extremist content and the facilitation of extremist relationships has grown exponentially. In fact, in 2016 alone, social media played a role in the radicalization processes of nearly 90% of the extremists in the PIRUS data.
- Lone actors (i.e. individuals who were operationally alone in their extremist activities) in the PIRUS data were particularly active on social media. From 2005-2016, social media played a role in the radicalization and mobilization processes of 68.12% of the lone actors in the PIRUS data. In 2016 alone, social media factored into the radicalization and mobilization processes of 88.23% of the lone actors in the PIRUS data. By comparison, from 2005-2016, social media factored into the radicalization of 50.15% of individuals who were members of extremist groups or radical cliques.
- Despite the increased usage of social media among U.S. extremists, user-to-user communications do not appear to increase the likelihood that extremists will be successful in traveling to foreign conflict zones or committing acts of domestic terrorism. In fact, the extremists who were most active on social media had lower success rates regarding foreign fighter travel and terrorist plots than individuals who were not as active on social media. Importantly, activity on open social media platforms, such as Facebook and Twitter, played a key role in the identification and interdiction of U.S. foreign fighters and terrorism suspects in several recent cases.
- While social media does not appear to increase the success rates of extremist outcomes, evidence suggests that it has contributed to the acceleration of radicalization of U.S. extremists. For example, the average radicalization duration (i.e., the time from first exposure to extremist beliefs to participation in extremist acts) of U.S. foreign fighters in 2005, when social media was first emerging as a factor in the radicalization of U.S. extremists, was approximately 18 months. In 2016, when over 90% of U.S. foreign fighters were active on social media, the duration of radicalization was down to 13 months on average.

[1] We define social media in the PIRUS dataset as any form of electronic communication through which users create online communities to share information, ideas, personal messages, and other content, such as videos and images. This form of online communication is distinct from other types of internet usage in that it emphasizes online user-to-user communication rather than passively viewing content hosted by an online domain. Additionally, our definition of social media does not include file-sharing sites (e.g., Torrent networks, Dropbox, P2P networks, etc.).

ABOUT THE PIRUS DATASET

Profiles of Individual Radicalization in the United States (PIRUS) is a database of 1,867 Islamist, far-left, far-right, and single-issue extremists who radicalized to violent and non-violent extremism in the United States from 1948 through 2016. The data used in this research brief are limited to individuals whose first publicly known extremist behavior (typically the date of their arrest or plot) took place between 2005 and 2016, and contained valid (i.e., non-missing) data for their social media usage as it related to their radicalization and/or mobilization processes. More information regarding the PIRUS dataset, including inclusion parameters, can be found at: http://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus.

FREQUENCY OF SOCIAL MEDIA USE

Between 2005 and 2016, social media played a primary or secondary role[2] in the radicalization[3] and/or mobilization[4] processes of 265 of the 479 (55.3%) extremists in PIRUS with valid data. These individuals used social media platforms in a wide variety of ways, including to consume and spread extremist narratives, create sharable content, and/or communicate with like-minded individuals.

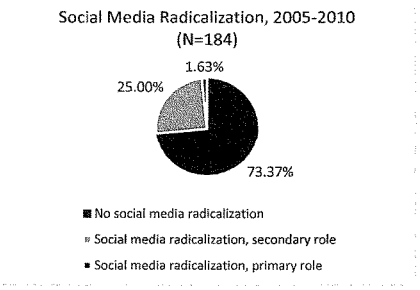


Figure 1

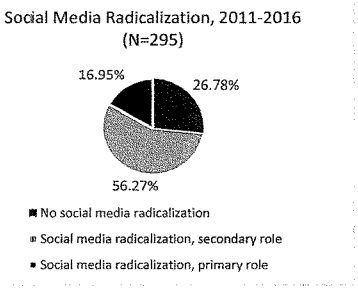


Figure 2

- From 2005 to 2010, only 49 out of 184 extremists displayed evidence of using social media in their radicalization or mobilization processes. However, of the 135 extremists who did not use any social media during their radicalization or mobilization processes, 24 (17.7%) of them interacted with other forms of online media, such as forums or message boards, and 22 of them (16.3%) utilized some form of non-internet media (e.g., music, videos, books, pamphlets, etc.).
- Merely 3 of these individuals (1.63%) from 2005 to 2010 utilized social media as their primary means of interacting with their affiliated extremist movements. The remaining 46 (25.00%) used social media as a secondary means of extremist interaction, instead favoring in-person relationships and other types of non-social media online communications, including chatrooms and online forums (Figure 1).

---

[2] We determined social media as playing a primary in the radicalization of individuals if their exposure to extremist ideologies and 50% or more of their socialization within extremist movements took place on social media platforms. Similarly, we determined social media as playing a secondary role in the radicalization of U.S. extremists if social media platforms were used to reaffirm or advance pre-existing extremist beliefs that were first acquired through face-to-face relationships. Finally, individuals were coded "No" for the influence of social media on their radicalization if they were present on social media sites but there is no indication that those sites contributed to their radicalization or mobilization.

[3] We define radicalization as the psychological, emotional, and behavioral processes by which an individual adopts an ideology that promotes the use of violence for the attainment of political, economic, religious, or social goals.

[4] We determined social media as playing a role in the mobilization of U.S. extremists if user-to-user platforms were used to plan, finance, or conduct extremist activities, including foreign fighter travel, non-violent illegal actions, and violent terrorism plots.

- In the last several years, however, social media has become a nearly ubiquitous method for consuming and sharing extremist content and communicating with extremists from around the world. From 2011 to 2016, 216 out of 295 (73.2%) of the extremists in PIRUS used social media platforms to passively consume content, participate in extremist dialogues, spread extant extremist propaganda, or communicate with other extremists (Figure 2).
- It should be noted that 166 out of the 216 (76.9%) extremists in PIRUS who used social media as part of their radicalization processes during this period used these platforms as a way to supplement existing face-to-face extremist relationships and participation in closed, offline extremist networks (Figure 2).
- Of the 295 extremists in PIRUS from 2011-2016, 50 relied primarily on social media as a means of radicalization (16.9%), indicating a substantial rise in the importance of social media as a way to consume content and communicate among extremists (Figure 2).

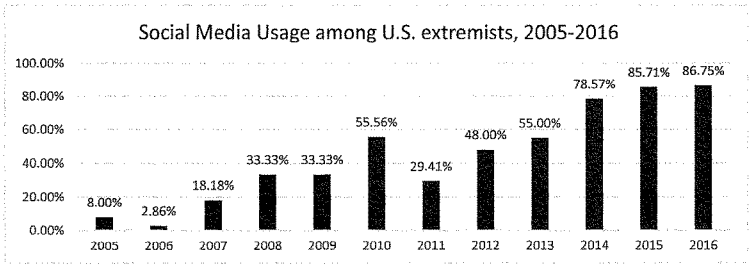


Figure 3

- As is expected when taking into account the exponential growth of social media, user-to-user platforms have factored into the radicalization and mobilization of a far greater percentage of U.S. extremists in recent years. In fact, in 2016 alone, social media played a primary or secondary role in the radicalization processes of 86.75% of the extremists in PIRUS, compared to only 48% four years prior (Figure 3).

SOCIAL MEDIA USAGE ACROSS DIFFERENT EXTREMIST TYPES – IDEOLOGICAL COMPARISONS

	Far-right	Far- left	Islamist	Single Issue
Yes, secondary role	40.69%	36.67%	48.10%	35.71%
Yes, primary role	2.07%	0.00%	19.08%	0.00%
No evidence of social media usage	57.24%	63.33%	32.44%	64.29%

Table 1

- Islamist extremists in the PIRUS data from 2005-2016 displayed the highest rates of social media usage and were the only ideological category in which a majority of cases utilized social media in their radicalization and/or mobilization processes (67.55%) (Table 1).
- In 2016, social media played a primary or secondary role in the radicalization of 93.18% of Islamist extremists in PIRUS.
- From 2005-2016, Islamist extremists were, by a large margin, the group most likely to engage with social media as a primary means of consuming extremist content or communicating with other extremists. In 2016, social media was the primary means of radicalization for 45.4% of the Islamist extremists in PIRUS. By comparison, individuals associated with extremist far-right, far-left, and single-issue movements most frequently used social media to supplement face-to-face or group-based radicalization processes (Table 1).

- From 2005-2016, far right extremists displayed the second highest rates of social media radicalization/mobilization (42.76%), although only 2.07% of far-right extremists during this period used social media as their primary means of radicalization (Table 1).
- Social media had the smallest impact on the radicalization processes of far left and single-issue extremists in the PIRUS data. From 2005-2016, social media was a secondary means of radicalization for 36.36% of far left and 35.71% of single issue extremists in PIRUS. Further, during this period, there were no instances where social media was the primary means of radicalization for far left or single-issue extremists (Table 1).

SOCIAL MEDIA USAGE ACROSS DIFFERENT EXTREMIST TYPES – GROUP ACTORS AND LONE ACTORS

From 2005-2016, social media played a notably larger role in the radicalization processes of lone actors than it did in the radicalization of extremists who were affiliated with extremist groups or radical cliques. During this period, social media played a role in the radicalization of 68.12% of the lone actors in PIRUS. By comparison, social media factored into the radicalization trajectories of just over half (50.15%) of group actors during this period (Figure 4).

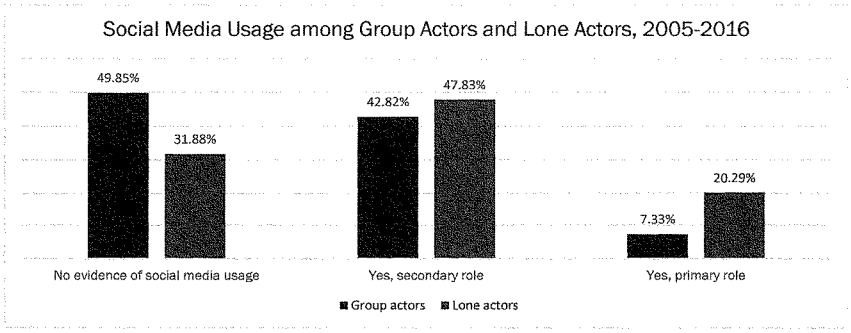


Figure 4

- In 2016 alone, social media factored into the radicalization and mobilization processes of 88.23% of the lone actors in the PIRUS data, while it factored into the radicalization of 76% of individuals who were members of extremist groups or radical cliques (i.e. non-lone actors).
- Furthermore, social media played a primary role in the radicalization of a substantial number of lone actors in PIRUS. Over one-fifth (20.29%) of the lone actors in PIRUS from 2005-2016 used social media as their primary means of radicalization, while only 7.33% of group actors primarily radicalized through social media use during this period (Figure 4).

SOCIAL MEDIA PLATFORMS

From 2005-2016, the extremists in PIRUS used a wide range of social media platforms within the context of radicalization and mobilization, including commonly used non-encrypted platforms designed for users to easily share and produce content, as well as lesser-used platforms that are used primarily for encrypted peer-to-peer communications.

- The types of social media platforms utilized most often by extremists in the PIRUS dataset largely reflect the mainstream popularity of the platforms in the United States.

- As the most popular social media platform in the United States,[5] Facebook was also the platform most commonly used by extremists in the PIRUS dataset. Nearly two-thirds of extremists (64.53%) used Facebook for radicalization or mobilization between 2005 and 2016 (Figure 5).
- YouTube was the second most frequently used platform among extremists, with a usage rate of nearly one-third (30.57%). The third most popular social media platform was Twitter, which was utilized by nearly a quarter (23.4%) of extremists in the data (Figure 5).
- From 2005 to 2016, over 10% of extremists used an encrypted platform, including Telegram, Kik, WhatsApp, and other encrypted platforms (Figure 5).
- However, it is likely that as mainstream social media services (e.g., Facebook, YouTube, Twitter, etc.) continue to improve their capability to quickly detect extremist content, more extremists will move to less well-resourced and/or encrypted platforms in an effort to share content, engage with others, and increase their operational security.

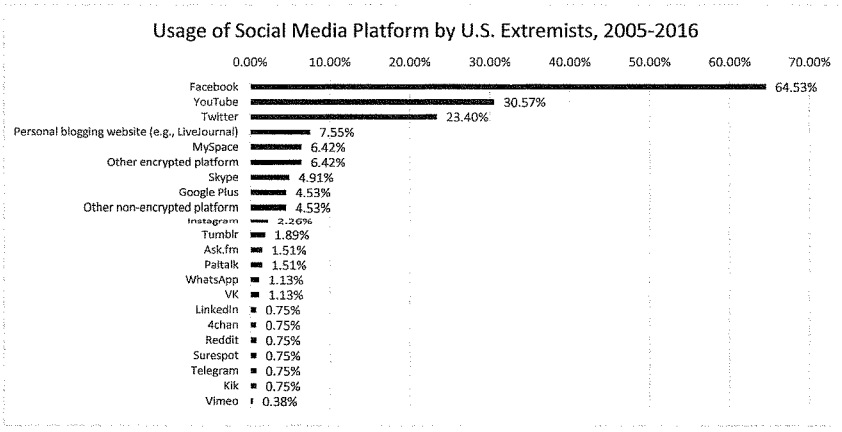


Figure 5

SOCIAL MEDIA ACTIVITIES[6]

US-based extremists use social media for a wide range of activities, most commonly viewing and sharing content.

- Of the 265 extremists who used social media between 2005 and 2016, 243 (91.70%) *at least* consumed extremist content passively, meaning they watched videos or read texts but may not have actively contributed any content themselves (Figure 6).
- A majority of the individuals in PIRUS used social media beyond simple content consumption; 155 (58.49%) disseminated content (e.g. shared or spread content) and 152 (57.36%) participated in extremist dialogues.
- By contrast, a much smaller proportion of individuals used social media to facilitate extremist activities. Fifty-five individuals (20.75%) created content, such as videos, manifestos, or journal entries, that justified and encouraged extremist acts.

[5] http://www.pewinternet.org/2016/11/11/social-media-update-2016/
[6] We conceptualized the range of social media activities as an ascending scale, where each successive activity is considered a more extensive use of social media in radicalization and/or mobilization.

- Slightly more (56 individuals; 21.13%) actively established relationships with other extremists using social media platforms. Finally, a small handful of individuals used social media to directly facilitate either travel to a foreign conflict zone (46 individuals; 17.36%) or a domestic terror plot (24 individuals; 9.06%).[7]
- Far-right extremists participated in extremist dialogues at a greater rate (67.74%) than far-left (54.55%) and Islamist (55.37%) extremists. Far-right extremists were also substantially more likely to actively create content (30.65%) than far-left (18.18%) and Islamist extremists (15.82%).
- During this period, U.S. extremists rarely used social media to facilitate domestic terror attacks (9.06%). Of those individuals who did use social media to help plan a domestic terror plot, 11 were far-right extremists, 10 were Islamist extremists, and 2 were far-left extremists.
- Islamists were far more likely to use social media to facilitate travel to a foreign conflict zone than to plan a domestic terror attack (25.99% compared to 5.65%). Islamist extremists also more commonly used social media platforms to establish a relationship with like-minded individuals (24.86%).

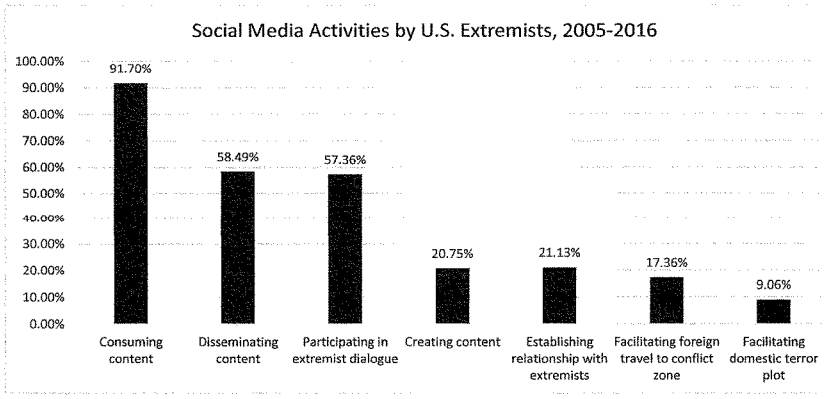


Figure 6

SOCIAL MEDIA USAGE AND EXTREMIST BEHAVIOR

	Used social media (N=265)	Did not use social media (N=214)
Involved in non-violent domestic extremist activities only (N=137)	40.15%	59.85%
Involved in violent domestic extremist activities (N=226)	52.22%	47.78%
Involved in foreign fighting only (N=116)	79.32%	20.68%

Table 2

- When comparing the social media usage of extremists who were involved in violent domestic plots, those who were involved in non-violent domestic illegal activities only, and individuals who only traveled or sought to travel to foreign conflict zones from 2005-2016, notable differences emerge. For example, of the 226 individuals who were involved in acts of violence or had clear intent to engage in violence in the United States (but may have been interdicted before violence was carried out), 118 (52.22%) radicalized or

[7] These figures include both successful and unsuccessful travel and/or attacks.

mobilized through the use of social media. By comparison, the majority (59.85%) of individuals who limited their extremist activities in the U.S. to non-violent crimes (e.g., financial crimes, property damage, and sending supplies and material to foreign terrorist groups) were not active on social media. Finally, of the individuals who left or sought to leave the United States to travel to an overseas conflict and were not involved in any violent or non-violent behavior with a domestic focus, 79.32% were active on social media (Table 2).

- The lack of social media usage was rare among foreign fighters in the PIRUS data, with only 24 (20.68%) avoiding social media platforms between 2005-2016 (Table 2). Indeed, every individual who left or attempted to leave the U.S. to join a foreign conflict in 2016 used social media as part of their radicalization and/or mobilization processes.

SOCIAL MEDIA ACTIVITIES AND PLOT SUCCESS

Among extremists who were involved in domestic terror plots, actively using social media platforms to communicate with other extremists in order to facilitate attacks was negatively associated with plot success.

- Only 10% of individuals who used social media to plan, finance, or conduct domestic terror attacks successfully carried out their plots.
- Inversely, individuals who used social media platforms for more passive uses during their radicalization and mobilization processes (i.e., consuming content, sharing content, participating in extremist dialogue, creating content, and communicating with other extremists for ideological knowledge), were significantly more likely to achieve plot success (33.67%).
- However, the data show that the most successful extremists in terms of plot progression abstained from using social media altogether. Indeed, individuals who were not present on social media had the highest rate of successful plots at nearly 36% (Figure 7).

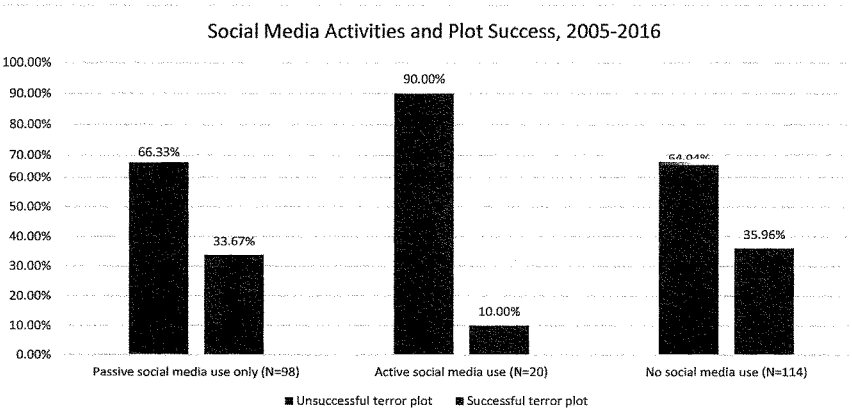


Figure 7

SOCIAL MEDIA USAGE AND FOREIGN FIGHTER SUCCESS

The evidence from the PIRUS data indicates that social media use is also inversely related to achieving success as a foreign fighter, understood here as traveling to a foreign conflict zone and joining a foreign non-state armed group. Among the 116 individuals in PIRUS from 2005-2016 who aspired to travel to a foreign conflict zone (but were not involved in a domestic terror attack), 68 ultimately failed to reach their destination. Of those, 56 (82.35%) were active social media users. By contrast, of the foreign fighters who did not use social media, 50% succeeded in their efforts (Figure 8).

- This finding carries over to individuals who used social media to establish relationships with travel facilitators on social media. Of the 48 individuals in PIRUS who aspired to be a foreign fighter (but were not involved in a domestic terror attack) and successfully reached a conflict zone, 36 (75%) did not have the help of an online travel facilitator or someone they thought was a facilitator. By contrast, 70% of the individuals who connected with online travel facilitators failed to reach their destinations (Figure 9).
- These findings support the conclusion that while social media is a powerful way for extremists to share ideas and communicate, the use of open platforms may leave individuals vulnerable to identification and interdiction by law enforcement.

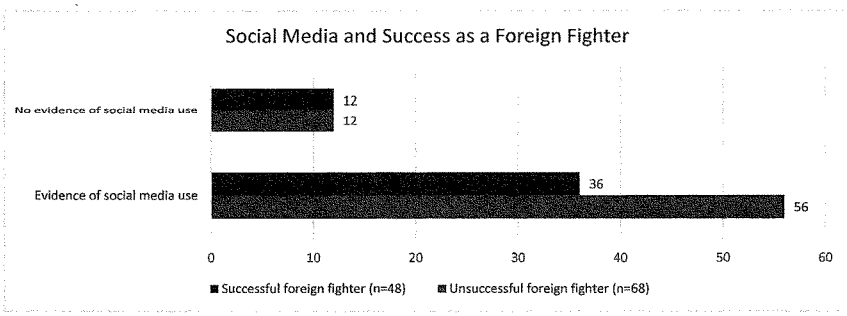


Figure 8

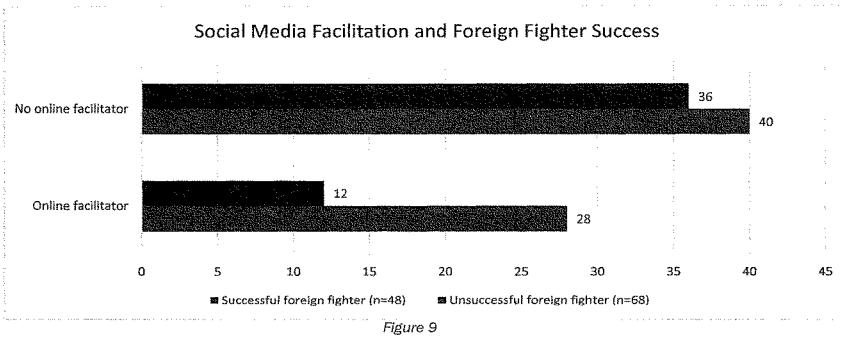


Figure 9

SOCIAL MEDIA USAGE AND RADICALIZATION DURATION

While social media usage does not appear to be linked to successful foreign fighter travel or domestic terrorism, preliminary evidence suggests that extensive social media use may accelerate the radicalization process. As social media usage has become nearly ubiquitous among extremists, the average duration of the radicalization process for some has shortened considerably. For example, among US-based foreign fighters in the PIRUS data, the average amount of time that elapsed between their first exposure to extremist beliefs and their first attempts to travel to foreign conflict zones decreased from approximately 18 months in 2005 to 13 months in 2016 (Figure 10). Although the average radicalization duration varies considerably from year to year, the overall trend has seen a gradual decrease in the amount of time spent prior to mobilization. These data support the findings of others (e.g., Carley, 2017) that social media usage in extremist movements accelerates consensus on radical viewpoints and increases commitment to the movements' objectives.

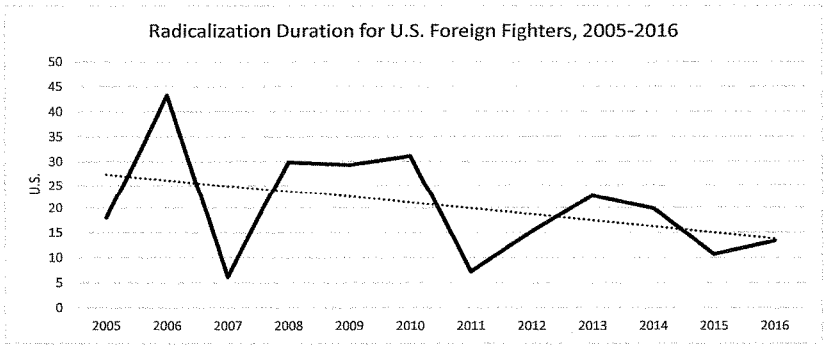


Figure 10

POLICY IMPLICATIONS

- Social media has become an increasingly important tool for extremists to disseminate content, share ideas, and facilitate relationships. Successfully mitigating the threat posed by homegrown violent extremists (HVEs) and domestic terrorists will require strategies for countering extremism online. These strategies must go beyond content removal and account deactivation to include leveraging social media to promote counter and alternative narratives and support services. Leveraging the newly established Global Internet Forum to Counter Terrorism (GIFCT) and identifying other ways to enhance the security of newer and less well-resourced online platforms will be a key to successfully devising and employing a comprehensive online counterterrorism strategy.
- While the conditions that allow for successful terrorist attacks are complex, preliminary evidence suggests that there is not a link between extensive social media use and the likelihood of carrying out a successful attack. In fact, the use of open social media platforms appears to make terrorist suspects vulnerable to law enforcement identification and interdiction.
- As open platforms, like Facebook and Twitter, continue to target extremist content for removal, individuals who adhere to radical ideologies are likely to continue their shift to secure social media services and lesser known platforms that are not as closely monitored. This shift could make it more difficult for law

enforcement to identify concerning online behaviors. Working with the GIFCT, governments should continue to assist smaller social media platforms in making their services less accessible to extremist groups.

- Given that social media use is positively correlated with unsuccessful plots and unsuccessful foreign fighter travel, due in part because social media usage leads to law enforcement disruptions, a strategy that relies on content and account takedowns may have the unintended effect of undermining counterterrorism investigations.
- While there does not appear to be a link between social media use and the successful commission of terrorist attacks in the US, increased social media activity may accelerate the radicalization process for some extremists. As individuals continue to gravitate to extremist content and dialogues online, and as the number of encrypted platforms proliferates, the windows of opportunity for intervening to off-ramp individuals who have begun to radicalize may continue to close rapidly. Thus, quickly identifying individuals who have begun to radicalize and providing needed support services will be a key component of a successful counterterrorism approach moving forward.

REFERENCES

Archetti, C. (2015). Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age. Perspectives on Terrorism, 9(1). Retrieved from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/401

Carley, Kathleen. (2017). Social Influence, Bots, and Fake News. Presentation to the Security, Networks, and Social Computing Working Group.

Cohen, K., Johansson, F., Kaati, L., & Mork, J. C. (2014). Detecting Linguistic Markers for Radical Violence in Social Media. Terrorism and Political Violence, 26(1), 246–256. https://doi.org/10.1080/09546553.2014.849948

Conway, M. (2017). Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. Studies in Conflict & Terrorism, 40(1), 77–98. https://doi.org/10.1080/1057610X.2016.1157408

Farwell, J. P. (2014). The Media Strategy of ISIS. Survival, 56(6), 49–55. https://doi.org/10.1080/00396338.2014.985436

Klausen, J. (2015). Tweeting the jihad: social media networks of Western foreign fighters in Syria and Iraq. Studies in Conflict & Terrorism, 38(1), 1–22.

PROJECT TEAM

Principal Investigator: Michael Jensen
Project Manager: Patrick James
Other Project Researchers: Gary LaFree, Aaron Safer-Lichtenstein, Elizabeth Yates

START

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is supported in part by the Science and Technology Directorate of the U.S. Department of Homeland Security through a Center of Excellence program led by the University of Maryland. START uses state-of-the-art theories, methods and data from the social and behavioral sciences to improve understanding of the origins, dynamics and social and psychological impacts of terrorism. For more information, visit www.start.umd.edu.

This project was supported by the Department of Homeland Security Science and Technology Directorate's Office of University Programs through Award Number 2012-ST-061-CS0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the National Institute of Justice or the U.S. Department of Homeland Security.

Use of social networks among the Palestinian public - Data and Insights

The Information Center for Intelligence and Terrorism named after General Meir Amit

at the Intelligence Heritage Center - MLM

The IPOKE company, a Palestinian company from Gaza that deals mainly in the field of digital marketing, and network research has published for the seventh year an annual report about the "digital reality in the territories of Palestine". The report, which refers to the year 2022, examines the consumption habits of the Palestinian public on social networks according to various segments such as age, place of residence, gender, times of activity on the network and more. The information mainly refers to Palestinians in Judea, Samaria and the Gaza Strip, sometimes it also refers to Israeli Arabs (IPOKE company report for 2022, IPOKE company website January 1, 2023). According to the company, the analysis of the information began at the beginning of 2022 and ended on December 25, 2022. The information is a combination of quantitative information obtained from questionnaires distributed by the company in order to measure social behavior and qualitative information obtained from the analysis of the information and the manual collection of data from social media platforms such as, LinkedIn, Telegram, and WhatsApp that do not have their own measuring factors.

The authors of the study testify that they encountered a number of problems, among them, difficulty in collecting the information.

One of the most important findings in the report **is the fact that the Tiktok, Telegram, and WhatsApp applications have become extremely popular, and their use is very widespread among the young Palestinian generation and Palestinian society. Also, for the first time in two decades, the TikTok application has surpassed Google as a search engine, especially among the young generation.**

The company, which does not reveal many details about itself, and it is not clear who the target audience is for its research, recommends using the findings of the report to market the Palestinian issue in the international arena.

42.2% of the respondents indicated that social networks are the most influential factor in mobilizing the public in favor of national issues in the domestic arena and improving the national image in the foreign arena, only 12.7% indicated the official media as the influential factor.

In accordance with these findings, attention should be paid to the popular apps and their contents and the degree of influence they have on the Palestinian public and especially on the younger generation:

- **Tik Tok**: It is widely used by children and teenagers. In this context, it will be mentioned that attacks were recently carried out by children aged 13-14, who were apparently influenced by the incitement expressed mainly on social networks. Tiktok is also used by the various organizations in the cities of Judea and Samaria during clashes with the IDF, to transmit messages between the activists and to transmit live reports from the field.
- **Telegram**: Used by older people and as a platform for transmitting information and messages among terrorist organizations such as the Jenin Battalion and the "Lions Den" organization, as well as messages to the public such as videos calling for terrorist attacks and even demonstrating how to carry them out.

- **WhatsApp**: Used for regular communication, visual information and to transmit messages, including "operational" ones.

The report findings

General

The report, which was published on January 1, 2023, examined seven million Palestinians in Judea, Samaria, the Gaza Strip and a few in Western Israel, which is approximately 5.5 million internet users on all devices. According to the Palestinian Telecommunications Company, there are approximately 4.4 million mobile phone subscribers (three million Joule, 1.44 million Ooredoo).

65.7% of the public use social networks. Among the users of social networks, 48.6% are women and 51.4% are men. The usage is according to the following division: 92% use Facebook, 90% WhatsApp, 81% YouTube, 67% Instagram, 38% Tiktok, 37%, Telegram, 26% Twitter, 17% LinkedIn, and 80.7% use chat rooms (voice chats).

In almost every age group, the use of women and men is similar, with a small advantage for men in some age groups, and for women in another. The use of social networks in general decreases as the age of the user is older. The most popular surfing hours are between 5 PM – 7 PM.

In response to the question of "what are the motivating factors for using social networking sites", the two most popular answers were: keeping up with the news and the need to contact family and friends. 42.2% indicated that social networks are the most influential factor in mobilizing the public in favor of national issues in the domestic arena and improving the national image in the foreign arena, only 12.7% indicated the official media as the influential factor.

The Social Networks

Tik Tok

The TikTok application is considered the most preferred in Palestinian society after the Corona epidemic, and the rate of its users is 38.2%. This platform is mainly used by the young age groups in the Palestinian public, the proportion of users aged 18-24 reaches 48% of all users. Among the users, 47.5% are men and 52.5% are women. These numbers correspond to Google's data according to which about 40% of the younger generation (Generation Z) prefer to use TikTok and Instagram.

According to the Palestinian Central Bureau of Statistics, Generation Z includes those in the age group of 15-29, numbering about one and a half million people, 897,000 in Judea and Samaria and East Jerusalem and 601,000 in the Gaza Strip. According to the authors of the report, the Tik Tok platform has gained popularity among the Palestinians, and it has been proven that it can cause a change in mindset and thanks to this, many supporters have joined it.

The use of TikTok in the Palestinian public according to age distribution:

- 18-24 – 77%

- 34-25 – 21%
- 35+ – 2%

For the first time in two decades, the TikTok application has surpassed Google as a search engine used especially by the younger generation. The younger generation uses this application because it is a simple application and the shortest way to get publicity, which does not require much effort. There is no need to register in the application to enter it and the children can enter it easily. In TikTok you can do everything, including shoot videos and get millions of views. The company's report emphasizes that, at the same time, TikTok also has negative aspects that may affect members of the younger generation because it is an application open to the whole world and it can be viewed and presented with various contents, including sexual and violent content. According to IPOKE, there is a lot of use of TikTok among the various organizations in the cities of Judea and Samaria and especially "Gov Aryot" because the application is not controlled and supervised by American officials (who usually monitor the contents). "Lion's Den" activists take advantage of this application to convey the Palestinian narrative to the younger generation and to acquire supporters and sympathizers for the Palestinian issue.

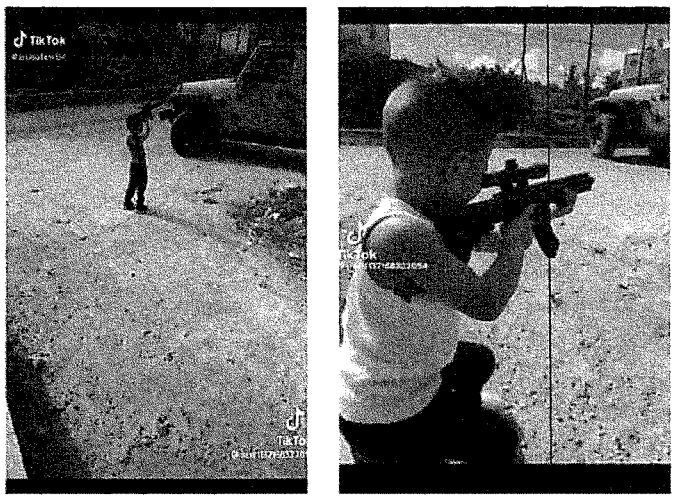
Considering this data, IPOKE states that it sees importance in social networks and their use as a means of spreading ideas in all fields. According to them, these measures can undoubtedly help to spread the Palestinian issue and gain support for it, as well as to raise a generation that is aware of its rights.

Below is the list of Palestinian hashtags and the number of views on them:

- Palestine, the capital of Al-Quds, 97.5 billion
- Palestine 95.4 billion
- Sharin Abu Aqla 175.3 million
- Lions' Den 63.1 million
- Resistance 58.2 million
- Jenin Battalion 10.7 million
- Jenin 3.4 billion views with 77% of them aged 25-34, 21% aged 18-24 and 2% aged 35 and over.
- Nablus (Nablus) 2.4 billion 76% aged 25-34, 22% aged 18-24 and 2% aged 35 and over.

Examples of incitement content distributed on the various social media platforms

Tik Tok:



Images from a video that circulated show children shooting toy weapons at a military vehicle

A performance in a kindergarten in Hebron in which the children show the burial of a martyr's body

Telegram

Recently, a collective transition of the Palestinians from WhatsApp to the Telegram application has been evident. Many residents of Judea and Samaria and the Gaza Strip have moved to this platform. The transition occurred due to a number of reasons including the restrictions imposed on Palestinian content on other platforms, technical problems and information security problems existing in the applications of the Meta company.

The number of Telegram users in Palestinian society currently stands at approximately 37.3% of all Internet users. Telegram enjoys the uniqueness of security and is difficult to hack. Telegram also does not limit the content to the user and does not censor them. Moreover, the sender of the messages can set a time limit for the message and order its destruction after a period of time. Over 80% of users believe that the Telegram application provides security and confidentiality when sending messages. In light of this, the IPOKE company recommends using the Telegram channels to publish the Palestinian narrative around the world.

Notable Telegram apps:

- Gaza Now: about 343 thousand followers.
- Jenin Al-Qasam: about 296 thousand followers
- "Lion's Den": about 234 thousand followers
- QUDSN network (which opposes the PA): about 215 thousand followers.

Due to these advantages and due to the widespread use of the application, we have found several examples where the Telegram channel has been used recently mainly by the organizations and terrorist organizations in Judea and Samaria.

In March 2023, media outlets affiliated with Hamas claimed that the Aqabat Jaber Battalion of Ezz Adin Al-Qassam (the military wing of Hamas) operating in the Aqabat Al-Jaber refugee camp near Jericho, was the one that confronted the IDF soldiers who entered the refugee camp. The battalion published a proclamation on the matter and even established a dedicated Telegram channel for its activity (March 1, 2023).

In the Palestinian-related tool, it was reported that after reports of the closure of the accounts of the organization "Gov Aryot" on Tik Tok and Instagram, following an appeal by Israeli officials to the management of the applications, there was an increase in the popularity of the organization on Telegram and within about 30 hours the number of its members jumped from about 60 thousand to 110 thousand .

Telegram serves as an important communication channel for the various organizations confronting Israeli security forces. Through Telegram, information is transmitted between activists who spread out at night in the streets and alleys of the cities and the refugee camps. The activists communicate with each other through encrypted conversations on the channel. According to one of the operators of the Jenin Battalion, Telegram is a relatively safe means and when problems develops and it is required to report on the progress of Israeli security forces, a message will be received via Telegram. The fighters also transmit information via Telegram about unfamiliar cars roaming the area and foreigners entering the camp (Frances24, April 13, 2022).

Online media outlets affiliated with Hamas recently published a video calling for "revenge attacks" against Jewish and Israeli citizens in public places. The video documents the so-called "next lone wolf", when he goes "to his death" in the street and suddenly murders Israeli citizens

and Jews (identified by anti-Semitic symbols such as wearing a kippa) using a gun and a knife by stabbing and slitting their throats. The video is accompanied by instructions for carrying out the revenge and was first uploaded on the Telegram channel that was opened, apparently, especially for that, but within a short time it was published in several official Hamas media outlets under the apparent claim that it was "spread on the Internet". A link to the video was published, among other things, on the Telegram channel of Al-Aqsa of Hamas.

Al-Arsala, a Hamas media outlet, recently posted on their Telegram channel at least two videos explaining and demonstrating how to "successfully" carry out attacks. One video talked about stabbing attacks (see above) and the other a video instructing how to carry out shooting attacks. The videos received a great response and widespread distribution.

The WhatsApp application is considered the most preferred instant messaging application among Palestinians. About 91% of the Palestinians in Judea and Samaria, the Gaza Strip and among Israeli Arabs use it. Among the users, 63% are women and 36% are men. The platform is popular mainly among 18-35 year olds. WhatsApp is one of the most famous and useful applications that allows its users to have a single conversation or a joint conversation. The application is free of charge and can be used for sharing photos, sound files, videos, direct location, as well as a channel for transmitting urgent messages.

Facebook

One of the leading platforms in Palestinian society even though its content is closely monitored. The rate of Facebook surfers stands at 92.9% of all internet surfers (the number also includes some Israeli Arabs). 51.4% of surfers are men and 48.6% women. 70% of surfers are academics, 26% have a secondary education. 72.9% use Messenger. Facebook Messenger is used by more women (53.2%) than men (46.8%). The age in which the highest number of surfers is 18-35. The prominent popular Facebook pages are mainly radio and television news pages.

Twitter

26.41% of all internet users use this platform. The report indicates that this is a figure that indicates an increase in the use of Twitter among Palestinian youth, especially in light of the campaigns to combat Palestinian content on other platforms. Among the surfers, 67% are women and 33% are men. The age groups in which the most widespread use are ages 18-24 (53%) and 25-34 (35%). Examining the prominent accounts shows that news site accounts on Twitter are less popular.

Instagram

It is a leading platform in Palestinian society for e-commerce needs. 67.5% of all Internet users use Instagram and it is one of the Palestinians' favorites. The women lead in its use (52.5%) compared to the men (47.5%). The age group that makes extensive use of the platform are 18-24 and 25-35.

YouTube

Plays an important role in general search operations and operations related to teaching and learning. The rate of surfers and subscribers stands at 81.8% (including among Israeli Arabs). Looking at the most popular channels among users, many children's channels come up.

- The IPOKE company was founded in 2016 with the aim of providing market research in the Palestinian area and over time expanded and began to operate also in the field of consulting and project implementation. The compary offers a variety of services in the field of internet marketing, product management, website development and design, business promotion, research and telemarketing (IPOKE website in Arabic, February 21, 2023).
- The company operates from Gaza, employs about ten employees (according to its LinkedIn website). The official website of the company does not indicate its place of residence except for the mention that it is from "Palestine". The phone that can be contacted is a mobile phone of the Palestinian cellular company Joel and its number is 0598478299 (and not a landline number that allows you to identify its location), the email address for contact is - info@ipoke.co (IPOKE website, February 21, 2023). Access to the company's IP is apparently blocked for security reasons. The company's website is published in Arabic only and the names of the company's managers and employees are not mentioned.

What is to blame for the involvement of Palestinian kids in terror attacks?

In Silwan, a 13-year-old boy opened fire at a group of Israelis, seriously injuring a father and his son. The attack took place in late January.

By KHALED ABU TOAMEH **Published:** FEBRUARY 16, 2023 19:16
Updated: FEBRUARY 17, 2023 08:10

HAMAS SUPPORTERS attend an anti-Israel rally in the northern Gaza Strip on Sunday.
(Photo credit: MOHAMMED SALEM/REUTERS)

Social media platforms, including TikTok, the popular Chinese short-form

"The children are influenced by videos and posts they see on social media," said Ibrahim Odeh, a political activist from east Jerusalem. "Every child has a smartphone or a computer, where they are exposed to all kinds of things."

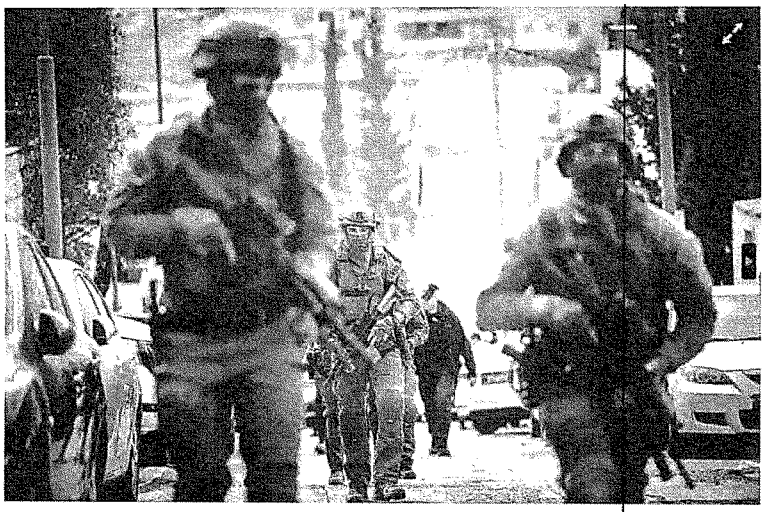
The involvement of three children aged 13 and 14 in the recent attacks in Jerusalem did not surprise many Palestinians, Odeh said. "The children watch videos of gunmen from Jenin and Nablus, and some want to be like them. They want to imitate the gunmen and other people who carry out attacks."

> **"The children are influenced by videos and posts they see on social media. Every child has a smartphone or a computer, where they are exposed to all kinds of things."**
> Ibrahim Odeh

y

vas

lling
in



SECURITY FORCES at the scene following the terror attack in the City of David, in eastern Jerusalem, last Saturday. (credit: YONATAN SINDEL/FLASH90)

In the past year, police have arrested dozens of teenagers on suspicion of participating in such attacks. Some were jailed; others were placed under house arrest.

In the past week, two children were involved in stabbing attacks in the Old City and the Shuafat refugee camp in northern Jerusalem.

In the first incident, an Israeli teenager was wounded. Police arrested a 14-year-old boy from the camp on suspicion of carrying out the attack. In the second incident, a 13-year-old boy, also from Shuafat camp, stabbed Border Police officer Asil Suaed, who was also accidentally shot by a civilian security guard, according to police. Suaed later succumbed to his wounds.

The three children who carried out the attacks in Jerusalem were not affiliated with any Palestinian faction. Rather, they acted as "lone wolves" after being

March 8, 2023

Senator Blumenthal
Chair
Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law
Washington, DC 20510

Senator Hawley
Ranking Member
Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law
Washington, DC 20510

Dear Chair Blumenthal and Ranking Member Hawley:

The more than three dozen undersigned public interest organizations, industry members, legal advocates, and academics share in the goal of a healthy, vibrant Internet, and we appreciate the time and energy the Subcommittee and its members have dedicated to this issue, including by holding today's hearing on "Platform Accountability: *Gonzalez* and Reform."

We are all invested in creating and supporting an Internet that works for everyone. We recognize that, like any tool that brings people together, bad actors can and do use the Internet to cause harm, and we want to be a resource as policymakers consider proposals to combat those harms. We are concerned, however, that ongoing conversations focused on Section 230 of the Communications Act (47 U.S.C. § 230) fail to account for the many ways that the law has empowered Internet users, including your constituents in states and communities across the country.

We believe that people finding and building communities is, by and large, a good thing. Through the Internet, people across the globe can discover and connect with each other at an unprecedented scale. This includes historically marginalized groups finding support and organizing, citizens participating in the democratic process, hobbyists connecting over niche shared interests, users providing reviews to hold institutions accountable, students and library

patrons engaging in online learning and research, and the everyday activity of staying in touch with loved ones. Section 230 makes this, and so much more, possible.

In policy conversations, Section 230 is often portrayed by critics as a protection for a handful of large companies. In practice, it's a protection for the entire Internet ecosystem. It is what enables anyone—from a multi-billion-dollar Internet company, to a small startup, to a non-profit, to a single Internet user—to create a space for communities to gather online. Because of Section 230, people have more ways, places, and opportunities to connect than ever before.

Absent Section 230's framework, anyone looking to host or reshare other people's expression would have to worry about a lawsuit—or just the threat of a lawsuit—any time one person wanted to silence another. Who would host or reshare remotely controversial content if they risked being sued for doing so? Given the high price tag of defending against, or even winning, a lawsuit, the vast majority of sites would be put in the position of hosting less user content or none at all. Websites would be effectively forced to either proactively screen user content before it could be shared or aggressively remove user content when anyone complains about it. Alternatively, some websites would scale back their moderation efforts to avoid liability, resulting in the proliferation of harmful content that would make those online spaces less productive. Ultimately, the result would be fewer places for communities to gather online and less expression, including fewer of the communities and less of the expression you support.

We are eager to be a resource in continuing conversations about improving the Internet, and we urge you to include in those conversations the perspective of Internet communities that have been made possible by Section 230.

Respectfully submitted,

Access Now
ACT | The App Association
American Civil Liberties Union
American Library Association
Association of Research Libraries
Authors Alliance
Center for American Entrepreneurship
Center for Democracy & Technology
Chamber of Progress
Computer & Communications Industry Association
Connected Commerce Council
Copia Institute
Consumer Technology Association
Developers Alliance
Educause
Electronic Frontier Foundation
Engine
Prof. Eric Goldman
Fight for the Future
Freedom House
INCOMPAS
Internet Infrastructure Coalition
Internet Society
Internet Works
IP Justice
NetChoice
New America's Open Technology Institute
OfferUp
Organization for Transformative Works
Patreon
PEN America
Progressive Policy Institute
Public Knowledge
R Street Institute
Software & Information Industry Association
TechFreedom
TechNet
Wikimedia Foundation

Cc: Members of the Subcommittee on Privacy, Technology, and the Law

○