THE DISINFORMATION BLACK BOX: RESEARCHING SOCIAL MEDIA DATA

HEARING

BEFORE THE

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

OF THE

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 28, 2021

Serial No. 117–31

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
45–497PDF WASHINGTON : 2022

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. EDDIE BERNICE JOHNSON, Texas, *Chairwoman*

ZOE LOFGREN, California
SUZANNE BONAMICI, Oregon
AMI BERA, California
HALEY STEVENS, Michigan,
Vice Chair
MIKIE SHERRILL, New Jersey
JAMAAL BOWMAN, New York
MELANIE A. STANSBURY, New Mexico
BRAD SHERMAN, California
ED PERLMUTTER, Colorado
JERRY MCNERNEY, California
PAUL TONKO, New York
BILL FOSTER, Illinois
DONALD NORCROSS, New Jersey
DON BEYER, Virginia
CHARLIE CRIST, Florida
SEAN CASTEN, Illinois
CONOR LAMB, Pennsylvania
DEBORAH ROSS, North Carolina
GWEN MOORE, Wisconsin
DAN KILDEE, Michigan
SUSAN WILD, Pennsylvania
LIZZIE FLETCHER, Texas

FRANK LUCAS, Oklahoma,
Ranking Member
MO BROOKS, Alabama
BILL POSEY, Florida
RANDY WEBER, Texas
BRIAN BABIN, Texas
ANTHONY GONZALEZ, Ohio
MICHAEL WALTZ, Florida
JAMES R. BAIRD, Indiana
DANIEL WEBSTER, Florida
MIKE GARCIA, California
STEPHANIE I. BICE, Oklahoma
YOUNG KIM, California
RANDY FEENSTRA, Iowa
JAKE LATURNER, Kansas
CARLOS A. GIMENEZ, Florida
JAY OBERNOLTE, California
PETER MEIJER, Michigan
JAKE ELLZEY, TEXAS
VACANCY

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

HON. BILL FOSTER, Illinois, *Chairman*

ED PERLMUTTER, Colorado
AMI BERA, California
GWEN MOORE, Wisconsin
SEAN CASTEN, Illinois

JAY OBERNOLTE, California,
Ranking Member
VACANCY
VACANCY

C O N T E N T S

September 28, 2021

THE DISINFORMATION BLACK BOX: RESEARCHING SOCIAL MEDIA DATA

TUESDAY, SEPTEMBER 28, 2021

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittee met, pursuant to notice, at 10:02 a.m., via Zoom, Hon. Bill Foster [Chairman of the Subcommittee] presiding.

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

HEARING CHARTER

The Disinformation Black Box: Researching Social Media Data

Tuesday, September 28, 2021
10:00 a.m. EDT – 12:00 p.m. EDT
Zoom

PURPOSE

The purpose of this hearing is to discuss how researchers are able to access and analyze data from social media companies. Researchers will testify about their work looking into the spread of misinformation and disinformation on social media platforms and how platforms drive traffic to advertisements and promoted posts. The hearing will also explore the limitations of current tools, techniques, and datasets for researching social media platforms and how researchers have utilized information available to advertisers to flag privacy concerns to the platforms. The hearing will examine how the Federal government can contribute to the ethical study of social media's impact on society while protecting the privacy of users.

WITNESSES

- **Dr. Alan Mislove**, Professor and Interim Dean, Khoury College of Computer Sciences, Northeastern University
- **Ms. Laura Edelson**, Ph.D. Candidate and Co-Director of Cybersecurity for Democracy at New York University
- **Dr. Kevin Leicht**, Professor, University of Illinois Urbana-Champaign Department of Sociology

OVERARCHING QUESTIONS

- What kind of data can and should be made available by social media companies in order to understand the spread of misinformation and disinformation and its impact on society?
- What kind of research is possible without privileged access to data from social media companies, and why is it important that researchers independent of social media companies have access to data?
- What are the limitations of current tools, techniques, and data sets used to analyze social media?
- What do we know about how misinformation and disinformation spreads on social media platforms and the effectiveness of platforms' monitoring and moderation techniques?
- How can the Federal government assist researchers in accessing data from social media companies that can help shed light on the spread of misinformation and disinformation?

Cambridge Analytica

The Cambridge Analytica scandal thrust into focus the issues of access to social media data for research purposes and the privacy breaches and political manipulation that ensued. Cambridge Analytica was a voter-profiling company that partnered with an outside researcher to collect data allegedly for academic purposes, but the data was in fact used in contracts with the 2016 presidential campaigns of Ted Cruz and Donald Trump.[1]

Cambridge Analytica harvested Facebook user data via personality quizzes. The quizzes were developed with an academic who got an app approved by Facebook on the basis that the data collected would be used for academic purposes. The app harvested data from users – informed about the collection via fine print – and from their Facebook friends, who were not informed. 270,000 users consented to participate in the personality quizzes and 50 million users' data were swept up in the collection, with 30 million containing enough personally identifiable information to create "psychographic profiles" incorporating records outside Facebook.

The U.S. Federal Trade Commission (FTC) initiated an investigation into Facebook in March 2018 following the allegations that Cambridge Analytica's actions violated a 2012 decree requiring notification when user data is shared beyond the agreed upon privacy settings.[2] The inquiry concluded in July 2019, when the FTC commissioners approved a $5 billion penalty for violating the 2012 order and established new accountability mechanisms for protecting user privacy, including an internal committee and compliance officers as well as biennial external assessors. The privacy requirements explicitly include third-party apps.[3]

State of the Available Data

A majority of Americans report using social media, with YouTube and Facebook drawing the eyes of 81 and 69 percent of Americans, respectively.[4] This makes social media platforms a wealth of information on individuals' habits, preferences, and beliefs. It also makes these platforms extremely valuable to advertisers – social media ad revenues totaled $41.5 billion in 2020.[5] Social media data is extremely valuable to researchers looking to understand what users are consuming on these platforms and how that content shapes their beliefs and behavior on- and offline.

The primary way social media platforms publicize data for public use is through Application Programming Interfaces (APIs). APIs are platforms on which companies publish data for use by third parties, including app developers, business partners, and researchers.[6] Researchers can write code that combs through the data available through the API, which they typically can gain access to after being verified by the platform.

---

[1] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html
[2] https://www.washingtonpost.com/news/the-switch/wp/2018/03/20/ftc-opens-investigation-into-facebook-after-cambridge-analytica-scrapes-millions-of-users-personal-information/
[3] https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions
[4] https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/
[5] https://www.cnbc.com/2021/04/07/digital-ad-spend-grew-12percent-in-2020-despite-hit-from-pandemic.html
[6] https://www.ibm.com/cloud/learn/api

APIs are limited in terms of data transparency because social media companies control what is shared and who has access. Researchers must also rely on social media companies to fix technical glitches when they occur. Researchers have expressed their desire for platforms to share more data and access, including items that advertisers have access to. This includes:

- the number of views on an ad (called "impressions");
- information on audience characteristics, such as gender;
- historical archives of advertisements beyond political ads;[7]
- the ability to run scripts to evaluate the vast contents of the Facebook Political Ad Library and other public databases provided by platforms; and
- information on how advertisements are targeted to specific individuals.

At the moment, only non-political advertisements that are currently running are available on Facebook's Ad Library. Political advertisements are available in the library for seven years, though Facebook itself classifies what qualifies as an ad about "issues, elections, or politics."[8] Furthermore, Facebook is making some impression data available in a quarterly report, but these reports show very little granularity, excludes impressions via private groups and pages, and only profiles the top 20 posts that were viewed in that period.

The tension between the public pressure to provide more data and the potential backlash on social media companies was exemplified in coverage of Facebook grappling with how to handle its CrowdTangle platform. CrowdTangle is a Facebook tool that provides access to public content on Facebook, Instagram, and Reddit. It allows third parties to track how and where public posts are shared and interacted with, though it does not provide access to impressions or demographics.[9] After journalists used the tool to show how frequently top performing posts originated from extremist and unreliable pages, some executives pushed a pivot to curated data sets, and reorganized the CrowdTangle team.[10] The CrowdTangle tool is still active, and Facebook has published curated data sets through its Facebook Open Research and Transparency (FORT) program.[11]

Facebook Revoking Access to Researchers

On August 4, Facebook revoked a team of New York University (NYU) researchers' access to the platform.[12] The researchers, including witness and PhD candidate Laura Edelson, were collecting data about political advertisements through a browser extension called the Ad Observatory. The extension had been running since September 2020. Volunteers downloaded the browser extension and consented to data collection on the political ads shown to them on

[7] https://blog.mozilla.org/en/mozilla/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like/
[8] https://www.facebook.com/help/259468828226154
[9] https://help.crowdtangle.com/en/articles/4201940-about-us
[10] https://www.nytimes.com/2021/07/14/technology/facebook-data.html
[11] https://research.fb.com/data/
[12] https://about.fb.com/news/2021/08/research-cannot-be-the-justification-for-compromising-peoples-privacy/

Facebook.[13] After Facebook issued a cease-and-desist letter in October,[14] the parties negotiated access terms for nine months and reached a standstill, at which point NYU turned its collection back on. Facebook then disabled the researchers' accounts, informing the team via an automated email message.[15]

Facebook alleges that the NYU team was engaging in unauthorized scraping that jeopardized the privacy of its users. Data scraping is when an automated program is used to collect information from another website or app.[16] The information can then be made available to third parties. Scraping itself is not inherently problematic. It is behind the tools we use every day, enabling search engines to deliver relevant results and price comparison tools to aggregate information across e-commerce platforms. Facebook's policy bans all unauthorized scraping, regardless of whether the data being accessed is widely available.[17] NYU researchers object to the characterization of their collection methods as scraping, saying that their extension collects only the ads seen by consenting users and not private information of users or their friends. Regardless of the particulars of NYU's research, scraping is a research technique that can be explicitly authorized by Facebook.[18] However, at the time it disabled the NYU researchers' accounts, Facebook posted a blog claiming that under its privacy program established pursuant to the 2019 post-Cambridge Analytica FTC order, the Ad Observer extension posed too serious a risk to user privacy, and opted to revoke researchers' access instead of authorizing the activity.

On August 5, the FTC sent a letter to Facebook noting that the action taken against the NYU researchers was not, in fact, required pursuant to the Facebook's consent decree with the FTC. The Acting Director of the Bureau of Consumer Protection noted that the FTC was not notified prior to Facebook's erroneous invocation of the decree. Furthermore, the letter explicitly condoned "good-faith research in the public interest" and noted Facebook's ability to make access exceptions to support such research.[19]

The dispute between Facebook and NYU serves as a helpful and timely illustration of the control Facebook has over the access researchers have to the platform. NYU's browser extension is still active and collecting data from users who have downloaded it, but the researchers' accounts remain locked, though Facebook has since acknowledged that this decision was not forced by the agreement with FTC.[20]

Algorithms

The transparency push on social media companies goes beyond user characteristics and ad impressions. Researchers are looking to understand how content reaches users. Along with the

[13] https://www.wsj.com/articles/facebook-cuts-off-access-for-nyu-research-into-political-ad-targeting-11628052204
[14] https://www.wsj.com/articles/facebook-seeks-shutdown-of-nyu-research-project-into-political-ad-targeting-11603488533
[15] https://www.nytimes.com/2021/08/10/opinion/facebook-misinformation.html
[16] https://www.targetinternet.com/what-is-data-scraping-and-how-can-you-use-it/
[17] https://about.fb.com/news/2021/04/how-we-combat-scraping/
[18] https://www.nytimes.com/2021/08/10/opinion/facebook-misinformation.html
[19] https://www.ftc.gov/news-events/blogs/consumer-blog/2021/08/letter-acting-director-bureau-consumer-protection-samuel
[20] https://www.wired.com/story/facebooks-reason-banning-researchers-doesnt-hold-up/

benefits of access to a near limitless amount of information, the Internet has also created information fatigue. To combat this and sell advertisements, social media platforms use algorithms to sort posts for users based on relevancy in order to prioritize which content a user sees and to increase the likelihood of the user engaging with that content. For example, Twitter, Facebook, Instagram, Reddit, TikTok, YouTube, Snapchat, and LinkedIn all create a personalized "feed"—also known as a timeline or newsfeed—from the content generated by the accounts followed by the user and/or the content the user has browsed previously. The choices that these algorithms make significantly dictate a user's experience. For example, a platform's algorithm may prioritize posts from user's friends, family, and groups to which they belong over sources of accredited news. Moreover, algorithms may place users in "filter bubbles" by only presenting content from like-minded people or amplifying selective exposure to information.[21]

The algorithms that make content decisions on social media are functionally black boxes, which means it is difficult to understand why algorithms make the decisions that they do. Training data is fed to the bottom layer of the algorithm's network, and as it passes through the succeeding layers it gets multiplied and added together in complex ways until it finally arrives at the output layer in its transformed final state. Due to the complex middle layers, observers can only effectively assess this process by reviewing an algorithm's inputs and outputs. Researchers and companies are working to improve algorithmic explainability, a topic of AI research that focuses on getting algorithms to explain their decisions, in contrast to the opaque "black box" model wherein even AI designers may not be able to track the AI's decision-making process. However, improving the explainability of algorithms has often come at the cost of accuracy of outputs.[22]

Researchers also lack the access necessary to study social media algorithms. This is in part because companies consider their algorithms to be trade secrets. Companies also benefit from the opaqueness of their algorithmic content decisions because they do not have to justify each decision. As a result, researchers are only able to assess certain outputs of social algorithmic curation, which has significantly limited this field of study. Even outputs are difficult to assess. For example, current tools offered by social media platforms do not allow researchers to retrieve the information that users see in their social feed in order to assess algorithmic choices. Similarly, confounding factors, such as the tendency of people to seek out others with similar preferences, make estimating the effects of algorithmic recommendations difficult to assess. As a result, researchers often must get creative to measure algorithmic effects, such as by using bots to create randomized field experiments.[23] Researchers looking into social media algorithms often conduct their studies without privileged access to platforms' data, putting out organic posts and paying for advertisements in order to track the metrics that are granted to paying customers but not researchers or ordinary users of the platforms.

The Spread of Misinformation and Disinformation

Many social media researchers focus on how misinformation and disinformation spread across platforms. Particularly since the 2016 Presidential election, when the public became aware of the impact of "fake news" on the broader political discourse, researchers have sought to examine

[21] https://5harad.com/papers/bubbles.pdf
[22] https://www.nature.com/articles/s42256-019-0048-x
[23] https://dl.acm.org/doi/fullHtml/10.1145/3447535.3462491

how untrustworthy information is spread, how platforms do or do not monitor and moderate it, and how it impacts society at large. A recent study found that on Facebook, publishers that share misinformation get six times as much engagement as trustworthy news sources.[24] While Facebook has pushed back and said that engagement data is not indicative of how many people view the misinformation relative to trustworthy posts, the company does not make impression data available to researchers.

Without more extensive data on the spread of misinformation and disinformation, it is difficult for third parties to assess how effective social media platforms' monitoring and moderation techniques are at managing dangerous content. A research group using Facebook's CrowdTangle tool found that pages sharing election misinformation tripled their interactions from October 2019 to October 2020, despite Facebook's partnership with third-party fact checkers to mark these posts as misinformation.[25] The same group used non-privileged access to Facebook to demonstrate the algorithm's push of anti-vaccine content via "related pages" suggestions.[26]

In July, the U.S. Surgeon General issued a report classifying misinformation as a public health threat, calling out the confusion over COVID-19 vaccines, preventative measures, and unproven treatments frequently stoked by malicious actors looking to profit financially or politically.[27] The report notes that health misinformation is not a new problem – it contributed to over 330,000 AIDS deaths between 2000-2005 – but that the changing information environment enabled by social media escalates the threat to unprecedented levels. Social media companies have pledged to combat misinformation and disinformation, taking steps like banning political advertisements around elections.[28] But it is imperative that third-party researchers who do not financially benefit from the spread of malicious content have sufficient access in order examine the potential threat of social media misinformation to public health and to democracy.

Ethics and Social Media Research

As with other forms of research focused on human subjects, the use of social media data in research poses important ethical concerns. To date, there is no clear consensus on an ethical framework for researchers entering this field like there is in other disciplines such as bioscience and health research. This situation is further complicated by the differing ways that social media platforms work with researchers as well as the ad hoc way in which disputes are resolved. As a result, different institutions and institutional review boards (IRBs) have created different guidance and recommendations for ethical social media research.

There are many ethical challenges regarding research that uses social media data, including privacy and consent, anonymity and confidentiality, authenticity of subjects, data security and management, and more. For example, informed consent can be difficult to acquire in social media research. In more traditional research approaches, informed consent is usually built into the research design, such as through consent forms. On the other hand, participants in social

[24] https://www.washingtonpost.com/technology/2021/09/03/facebook-misinformation-nyu-study/
[25] https://secure.avaaz.org/campaign/en/facebook_election_insurrection/
[26] https://secure.avaaz.org/campaign/en/fb_algorithm_antivaxx/
[27] https://www.hhs.gov/sites/default/files/surgeon-general-misinformation-advisory.pdf
[28] https://www.nytimes.com/2021/03/03/technology/facebook-ends-ban-on-political-advertising.html

media-based research are often unaware of their participation and do not give prior written, informed consent. While this consent may be given in the form of a platform's terms and conditions, ethical questions remain whether users truly read and understand these agreements. Similarly, anonymity is a key consideration in research ethics, particularly in qualitative research practices or when data sets are shared outside of the original research team.

Grant-making agencies, such as the National Science Foundation (NSF) and the National Institute of Health, have created numerous methods and procedures to allow for research in sensitive topics while protecting the privacy and security of research participants. One example of this is the NSF's National Center for Science and Engineering Statistics (NCSES), which has created numerous procedures for the data it licenses to researchers. Beyond directly funding research, agencies have had little direct involvement with opening secure access to social media data.

Chairman FOSTER. Well, the hearing will now come to order. Without objection, the Chair is authorized to declare recess at any time. And, before I deliver my opening remarks, I wanted to note that today the Committee is meeting virtually. I want to announce a couple of reminders to the Members about the conduct of the hearing. First, Members should keep their video feed on for as long as they are present in the hearing. Members are responsible for their own microphones. Please also keep your microphones muted, unless you're speaking. And finally, if Members have documents that they wish to submit for the record, please e-mail them to the Committee Clerk, whose e-mail address was circulated prior to the hearing.

Well, good morning, and welcome to our Members and our panelists. We've—I especially appreciate your willingness to have the hearing rescheduled to a time when nothing is happening in Washington, D.C. and Congress. But thank you all for joining us for this hearing on researcher access to social media data. For years experts have been raising the alarm about how misinformation and disinformation spreads unabated on social media platforms. Long before "fake news" was an epithet aimed at influencing—anything conflicting with someone's own worldview, it described falsehoods presented maliciously as fact in order to influence opinions. The problem of misinformation is not a new one, but social media has fanned the flames, and it is now difficult to imagine political and social discourse untouched by its influence.

The damage caused by misinformation reaches far beyond our phone and computer screens. Lies on social media have spawned riots and ethnic cleansing, and thousands of deaths around the world, and lies about the 2020 election inspired thousands to invade our Capitol on July—on January 6 in an attempt to disrupt our Constitution, and stop the certification of valid election results, resulting in five deaths. Lies about the severity of COVID–19 prevented millions of Americans from taking the disease seriously, resulting in needless infections and needless deaths. Vaccine disinformation is discouraging Americans from receiving safe and effective COVID–19 vaccines, extending the pandemic, and allowing new variants to proliferate.

For years we have seen the harmful effects of anti-vaccine rhetoric, causing the re-emergence of diseases like measles that had been eliminated by vaccines. In fact, in July the Surgeon General declared that misinformation on social media was a public health hazard. Much of this misinformation, in fact, appears to be generated and amplified by our enemies, who recognize the damage that it does to our country. It is therefore imperative that the Science Committee address it as we would any other threat to public health, by ensuring that we have the best and brightest minds researching the problem so that we can base future policy on the best available evidence.

Unfortunately, it's extremely difficult for researchers to gain sufficient access to social media data. Companies do make some information public, but it is largely through interfaces that they control, meaning that researchers can only see what the companies want them to see, and access can be cutoff at any time. Today we will hear from our witnesses about the research they are able to con-

duct in this environment. They will tell us about the limitations of the existing tools, and what data they believe can and should be made public so that we can have a better understanding of how social media users interact with misinformation, and how that impacts their behavior online and offline. We will hear about how mis- and disinformation is delivered to social media users through the black box of the algorithm, drawing eyes to the sensationalist content that inspires the most user engagement, regardless of truth.

We on the Science Committee understand that the very real limitations to full data transparency by social media is a real problem. Platforms will argue that some information should be protected as trade secrets, much as the computerized financial trading firms prize the opacity behind their sometimes abusive trading algorithms. At the same time, social media users are entitled to privacy, particularly of personally identifiable information. However, these concerns cannot be broad excuses to shield social media companies from a full outside accounting of how their platforms may be endangering public health and safety. We simply cannot leave social media unstudied. It is as influential a force on the social fabric of the 21st century as any other.

But as it stands, advertisers on these platforms often enjoy more access to data than academic researchers looking to access the impact of promoted posts. I believe that this—in this hearing we can have a constructive launching point to explore how the Science Committee can contribute to this conversation. We must strike a balance between protecting user privacy and confidential business information, while also acknowledging that objective, independent research is necessary to understand how these platforms influence modern society. We've solved this problem for electronic trading and financial services. We are solving this problem for academic access to electronic health records, and we must solve this problem here.

I look forward to hearing from our panelists about how we can support their important work of shining a light onto the disinformation black box that is poisoning our public discourse.

[The prepared statement of Chairman Foster follows:]

Good morning, and welcome to our members and our panelists. Thank you for joining us for this hearing on researcher access to social media data. For years, experts have been raising the alarm about how misinformation and disinformation spreads unabated on social media platforms. Before "fake news" was an epithet, aimed at anything conflicting with someone's worldview, it described falsehoods presented maliciously as fact in order to influence opinions. The problem of misinformation is not a new one, but social media has fanned the flames, and it is now difficult to imagine political and social discourse untouched by its influence.

The damage caused by misinformation reaches far beyond our phone and computer screens. Lies about the 2020 election inspired thousands to invade the Capitol on January 6 in an attempt to stop the certification of the election, resulting in five deaths. Lies about the severity of COVID-19 prevented millions of Americans from taking the disease seriously, resulting in needless infections and deaths. Vaccine disinformation is discouraging Americans from receiving safe and effective COVID-19 vaccines, extending the pandemic and allowing new variants to proliferate. For years we have seen the harmful effects of anti-vaccine rhetoric, causing the re-emergence of diseases like measles that had been eliminated by vaccines.

In July, the Surgeon General declared that misinformation on social media is a public health hazard. It is therefore imperative that the Science Committee address it as we would any other threat to public health—by ensuring that we have the

brightest minds researching the problem so we can base future policy on the best available science.

Unfortunately, it is extremely difficult for researchers to gain sufficient access to social media data. Companies do make some information public, but it is largely through interfaces they control, meaning that researchers can only see what companies want them to. And access can be cut off at any time. Today, we will hear from our witnesses about the research they are able to conduct in this environment. They will tell us about the limitations of the existing tools, and what data they believe can and should be made public so we can have a better understanding of how social media users interact with misinformation and how that impacts their behavior on- and offline. We will hear about how mis- and disinformation is delivered to social media users through the "black box" of the algorithm, drawing eyes to sensationalist content that inspires user engagement regardless of the truth.

We on the Science Committee understand the very real limitations to full data transparency by social media companies. Platforms will argue that some information should be protected as trade secrets. In addition, social media users are entitled to privacy, particularly of personally identifiable information. However, these concerns cannot be broad excuses to shield social media companies from a full outside accounting of how their platforms may be endangering public health and safety. We cannot simply leave social media unstudied. It is as influential a force on the social fabric of the 21st century as any other. But as it stands, advertisers on these platforms often enjoy more access to data than academic researchers looking to assess the impact of promoted posts. I believe that this hearing can be a constructive launching point to explore how the Science Committee can contribute to this conversation. We must strike a balance between protecting user privacy and confidential business information, while also acknowledging that objective, independent research is necessary to understand how these platforms influence modern society.

I look forward to hearing from our panelists about how we can support their important work shining a light into the disinformation black box poisoning our discourse.

I now yield to Ranking Member Obernolte for his opening statement.

Chairman FOSTER. And I now yield it to Ranking Member Obernolte for his opening statement.

Mr. OBERNOLTE. Well thank you very much, Chairman Foster, and thank you to our witnesses for being here at this very important hearing, and what will prove, I'm sure, to be a fascinating hearing on combatting the spread of misinformation on social media.

We live in an amazing world, a world where we are presented with a selected, curated newsfeed that only includes the things that we're personally interested in. And that's informed by algorithms that companies like social media have come up with to foster user engagement, and to maximize our interest in the information that's being provided. But, unfortunately, as the Chairman pointed out, that's also catalyzed the spread of misinformation. Combatting that spread is something that has been a societal problem for hundreds of years now, but it's exacerbated by the fact that information now spreads so easily, and that that information is personalized to each one of us. So the information that I see in the morning is not the same thing that—the information that other people see in the morning, and, unfortunately, that can hide and mask the spread of this misinformation.

And if you want a perfect example of how that can be problematic, you can look at a hearing that this Subcommittee held a couple of weeks ago on the origins of COVID. And one of the—for me, the very surprising outcomes of that Committee hearing was the fact that, although we had competing theories about the spread of COVID, that any theory other than natural zoonotic origin had been rejected early in the crisis as misinformation, and had been labeled a conspiracy theory, and that the social media companies

had actively suppressed the spread of that information. And now, with the benefit of hindsight, and the discovery of new data, we've discovered that competing theories are not only possible, but indeed plausible, and in fact, you know, might end up being the successful theory.

So no one can deny that this effort to combat the spread of misinformation has severely hampered our ability to identify the origins of COVID. And it just illustrates how these two ideas are in tension, right? On one hand, we want to be a society that honors the exercise of free speech, but that is fundamentally intentioned with the idea that we also have an obligation to stop the spread of misinformation. So I'm hopeful that some of our panelists today will be able to talk some more about where that moral boundary is.

And figuring out, as a society, how to balance those two competing interests, I think, is critical. Because on the one hand, as recent events have shown, we all have a vested interest in trying to figure out how to stop the spread of misinformation. But on the other hand, history has shown us repeatedly that if we allow censorship to take the place of misinformation, that will take us down a very dark path as a society. So we have to find this middle ground, this balance in between the two, and I'm confident that we can.

And I'm also confident that the social media companies, like Facebook, and Instagram, and Twitter, are going to be critical to helping us solve this problem, because they have the expert knowledge in the way their algorithms work, they have the expert knowledge in the way that this information spreads, and what catalyzes peoples' interest in news about the world around them. And so I think, definitely, that they're going to need a seat at the table. We're going to need to tap all of our available sources of information, which certainly includes them, but also includes the independent researchers we're going to hear from today, and I'm very thankful that they're out there, gathering this information, to give us a holistic view of this problem. So I am looking very much forward to the hearing, and looking forward to asking questions afterwards. Thank you, Mr. Chairman. I yield back.

[The prepared statement of Mr. Obernolte follows:]

Good morning. Thank you, Chairman Foster, for convening this hearing. And thanks to our witnesses for appearing before us today.

Misinformation is not a new phenomenon. Disinformation campaigns have been used throughout history to spread state propaganda and influence geopolitics. It is no secret that misinformation has the ability to change hearts and minds and influence perceptions. What is new is the impact that modern advances in information and communications technologies have had on the ability of misinformation to spread. It is easier now than ever before to reach global audiences, communicate instantaneously with friends and family around the world, and follow every move of politicians, athletes, and Hollywood stars alike.

The same technologies that facilitate and democratize global access to information also enable the dissemination of information at a scale and speed like we have never experienced before in human history. This has made it more difficult to determine the accuracy, provenance, and objective truth of the information we consume. There is more information presented to individual consumers than ever before, and from myriad different sources.

The tremendous growth in the popularity of social media platforms over the past decade has resulted in the consumption of information that is more personalized than ever before. The information we read and view online is now perfectly tailored to each of our own individual preferences, biases, and beliefs. We each receive an individualized, curated feed of information every time we visit our social media plat-

form of choice. And it would not be a stretch to say that, at times, we are each drinking from our own individual information firehoses.

In this golden age of information, there are many outstanding questions about how we can assess and ultimately combat the spread of falsehoods, untruths, "fake news," and misinformation. I'm pleased that each of the witnesses testifying before us today has undertaken research to learn more about how misinformation spreads, and what we can do to combat it. This is an admirable goal, and we in Congress must take steps to facilitate further research on this important topic. But these efforts cannot be undertaken without ensuring appropriate constraints, limitations, and safeguards are in place.

The need for data transparency and access is inherently in tension with the protection of user privacy. We must endeavor to strike a healthy balance between data transparency on the one hand, and the protection and preservation of individual privacy on the other.

We must also respect and protect the intellectual property rights of the platforms whose data researchers seek to access and analyze. Social media and technology platforms have invested significantly in the development of their processes, technologies, and algorithms, which in many ways is what distinguishes the user experience of one platform from that of the others. Each platform is in a race to do it better, faster, and for less than their competitors. And they rightfully take great pains to police and protect their trade secrets from public disclosure. An appropriate balance must be reached between the intellectual property rights of platforms and the desire to access and analyze their technologies, processes, data, and algorithms for the public benefit. I'm not suggesting that it's an easy balance to strike, but merely asserting that we must keep this in mind as we work forward.

There is no doubt that misinformation can have harmful and even deadly real-world consequences. State-sponsored actors from Russia and China have recently engaged, and continue to engage, in coordinated disinformation campaigns. From Russia's efforts to foment discord and chaos around American elections, to China's efforts to lay blame for COVID-19 at the feet of the American government, state-sponsored disinformation campaigns have real consequences.

While social media platforms have rightfully taken steps to thwart the spread of misinformation, they must also protect against overcorrection that results in censorship. Competing hypotheses about the origins of COVID-19 are a compelling example. For almost a year, the suggestion that COVID-19 could have originated from anything other than natural zoonosis was summarily dismissed as conspiracy theory by traditional and social media alike. However, data now suggests that other hypotheses are in fact more plausible, and only recently did mainstream and social media platforms cease to censor these theories. The censorship of competing explanations has unquestionably impeded important efforts to investigate the virus' origins.

Similarly, we must also leave room in our social and political discourse for parody, satire, and commentary. An appropriate balance is necessary to ensure that such commentary is not discouraged or inappropriately discarded as conspiracy theory or misinformation. Just as misinformation can have real-world consequences, so too can overcorrection that leads to censorship of public debate about different ideas.

Combatting misinformation is not an easy endeavor. And the many researchers looking at how misinformation spreads online and how to successfully thwart it should be praised for their efforts. But if we ever expect to truly solve this problem, then we must recognize that the social media platforms must have a seat at the table. We cannot expect them to go it alone, and we should likewise not expect to stop the spread of harmful misinformation without them.

We must also endeavor to determine how to balance our societal goal of minimizing the spread of misinformation with the competing goal of the avoidance of censorship. This balance is critical because, as history has so often shown, to empower our media with the unchecked ability to censure would lead our country down a very dark path.

I look forward to learning more from our witnesses about how we can work to combat the spread of misinformation on social media, while simultaneously protecting users' privacy, platforms' intellectual property, preventing overcorrection, and preserving public discourse.

Thank you, Chairman Foster, for convening this hearing. And thanks again to our witnesses for appearing before us today. I look forward to our discussion.

I yield back the balance of my time.

Chairman FOSTER. Thank you. And we are honored to have the Full Committee Chairwoman, Ms. Johnson, with us today. The Chair now recognizes the Chairwoman for an opening statement.

Chairwoman JOHNSON. Well, thank you very much, Mr. Chairman, and let me say good morning, and greet our panelists, and thank you for holding this hearing. The topic will only grow in relevance as social media becomes all the more ingrained in our lives. And worryingly, these issues will become more dangerous with every topic that becomes hotly politicized.

Disinformation has been a public health threat for decades. Experts estimate that 330,000 deaths from AIDS (acquired immunodeficiency syndrome) in the early 2000's can be attributed to disinformation about the connection between HIV (human immunodeficiency virus) and AIDS. The fact of human-caused climate change, with decades of empirical evidence and expert consensus behind it, has nevertheless become a subject of great debate. Monied interests fan the flames of doubt as oceans rise and forests burn. And now, as we conduct this hearing virtually due to a surge in COVID–19, conspiracy theorists and malicious actors spread lies about the severity of the pandemic. Laymen speculate wildly about the vaccine's safety, drowning out expert voices. Social media offers fertile ground for these falsehoods, and unfounded claims that can spread across the globe in the blink of an eye.

We must not leave the black box of social media disinformation unexamined. Navigating the difficulties in extending access to data will not be easy, but failing to do so will have devastating consequences. This current moment is a grave example of the stakes at hand. We will not beat the pandemic without increased vaccine uptake, and every day social media users are dissuaded from getting the shot after seeing deeply misinformed posts. People are making decisions for the health and safety of themselves, their families, and their communities based on abject falsehoods, and researchers determined to mitigate the damage are unable to access critical data on how these lies spread.

I am pleased to join you and others, Chairman Foster, in welcoming our witnesses today. They are doing important research into how misinformation circulates on land—online and impacts our real-world health and safety. I look forward to your testimony. I yield back.

[The prepared statement of Chairwoman Johnson follows:]

Good afternoon to our panelists, and thank you to Chairman Foster for holding this hearing. This topic will only grow in relevance as social media becomes all the more ingrained in our lives. And worryingly, these issues will become more dangerous with every topic that becomes hotly politicized.

Disinformation has been a public health threat for decades. Experts estimate that 330,000 deaths from AIDS in the early 2000s can be attributed to disinformation about the connection between HIV and AIDS. The fact of human-caused climate change, with decades of empirical evidence and expert consensus behind it, has nonetheless become a subject of great debate. Monied interests fan the flames of doubt as oceans rise and forests burn. And now, as we conduct this hearing virtually due to a surge in COVID-19 cases, conspiracy theorists and malicious actors spread lies about the severity of the pandemic. Laymen speculate wildly about the vaccine's safety, drowning out expert voices. Social media offers fertile ground for these falsehoods, and unfounded claims can spread across the globe in the blink of an eye.

We must not leave the black box of social media disinformation unexamined. Navigating the difficulties in extending access to data will not be easy, but failing to do so will have devastating consequences. This current moment is a grave example of the stakes at hand. We will not beat this pandemic without increased vaccine uptake, and every day, social media users are dissuaded from getting the shot after seeing deeply misinformed posts. People are making decisions for the health and safety of themselves, their families, and their communities based on abject false-

hoods. And researchers determined to mitigate the damage are unable to access crucial data on how these lies spread.

I'm pleased to join Chairman Foster in welcoming our witnesses today. They are doing important research into how misinformation circulates online and impacts our real-world health and safety. I look forward to hearing your testimony.

Chairman FOSTER. Thank you. And if there are Members who wish to submit additional opening statements, your statements will be added to the record at this point.

And at this time I'd like to introduce our witnesses. Our first witness is Dr. Alan Mislove. Dr. Mislove is a Professor, the Interim Dean at—and Interim Dean at the Khoury College of Computer Sciences at Northeastern University. His primary field of interest concerns distributed systems and networks, with a focus on using social networks to enhance the security, privacy, and efficiency of newly emerging systems.

VOICE. This is——

Chairman FOSTER. He is also a core faculty member of the Cybersecurity and Privacy Institute, which forges global partnerships with experts in industry, government, and academia.

After Dr. Mislove is Ms. Laura Edelson. Ms. Edelson is a Ph.D. candidate in Computer Science at NYU's (New York University's) Tandon School of Engineering. Laura studies online political communication, and develops methods to identify inauthentic content and activity. Her research has informed reporting on social media ad spending in several national papers, including the New York Times. Prior to rejoining academia, Ms. Edelson was a software engineer for Palantir and FactSet, with a focus on applied machine learning and big data.

Our final witness is Dr. Kevin Leicht. Dr. Leicht is a Professor and former Head of the Sociology Department at the University of Illinois Urbana-Champaign, and Director of the Iowa Social Science Research Center at the University of Iowa. That's some commute. He previously served as a Program Officer for the Sociology and Resource Implementations for Data Intensive Research—the Data Intensive Research Program at the National Science Foundation. He has written extensively on issues related to economic development, globalization, and political sociology.

As our witnesses should know, they each have five minutes for your spoken testimony. Your written testimony will be included in the record for the hearing. When you all have completed your spoken testimony, we will begin with questions. Each Member will have five minutes to question the panel. And now we will start with Dr. Mislove. Dr. Mislove provides his testimony. Proceed.

TESTIMONY OF DR. ALAN MISLOVE, PROFESSOR AND INTERIM DEAN, KHOURY COLLEGE OF COMPUTER SCIENCES, NORTHEASTERN UNIVERSITY

Dr. MISLOVE. Chairman Foster, Chairwoman Johnson, Ranking Member Obernolte, and distinguished Members of the Subcommittee, thank you for the opportunity to appear before you today. My name is Alan Mislove. I'm a Professor and Interim Dean at the Khoury College of Computer Sciences at Northeastern University. My research is on algorithmic auditing. I develop methodologies that allow me to study large online platforms, such as

those operated by social media companies, to better understand how they work, how they may be abused, and what impacts they are having on users. Importantly, I conduct my research independently, without companies' permission, and without insider access to data. Put simply, I have no more access to these platforms than any of you do.

This is a significant challenge. It is difficult to develop the technologies that enable my work, especially because companies are resistant to external accountability, and a work and legal environment that makes such research carry non-trivial risk. As social media platforms mediate an increasingly large fraction of online communication, independent research such as this is critical. Even in the best of worlds, understanding how these platforms are impacting end users and society is too big a task for the platforms themselves. Though much remains to be done, my group and collaborators have been successful at studying a variety of such platforms, identifying alarming behaviors, and working with platforms to make improvements. Thus, I am well-positioned to provide input on what can currently be measured, and what is needed going forward to ensure we fully understand the impact that platforms are having.

So that you can appreciate how we conduct our research, we typically study platforms using one of two approaches. We can recruit cohorts of users who agree to donate their data, or we can run our own experiments on the platforms, for example, by becoming an advertiser. Unfortunately, both of these approaches that we have today have significant limitations. Running our own experiments is often expensive in terms of time and money, requires significant expertise, and is beyond the capabilities of many researchers and regulators. Worse, platforms often actively try to prevent such data collection, have suspended researchers' accounts, and have threatened litigation for ethical research in the public interest, with a notable exception—example being one of my fellow witnesses.

Platforms may say that researchers can rely on aggregated data that they provide, but this statement is misleading at best. Social medial platforms have been very hesitant to release any data, and have often only released aggregated coarse-grain data in the face of scandal and public backlash. Often, even accessing the data they do release can be challenging. In many cases, data sets require approval from the platform to be able to access, and cannot be shared with other researchers. Moreover, recent events have shown that platforms cannot be trusted to provide even correct aggregated data. It was recently revealed that Facebook neglected to include data from half of the U.S. population, one of the data sets it provided, calling numerous studies that relied on that data set into question.

The upshot is that currently no regulations exist that require platforms to make data available, and platforms are actively attacking independent researchers' ability to study their impacts. In effect, researchers are relying on platforms' goodwill to allow studies to be run at all, a situation that is becoming less and less tenable as platforms become more entrenched. Thus, my key message is that researchers need Congress to enshrine into law require-

ments for platforms to make data available. Mandating such transparency requires nuance, but is both feasible and urgent.

In particular, I want to convey three key considerations for how to shape such requirements. First, social media platforms sit inside broader sociotechnical systems, and the data that regulations requires be made available must be comprehensive enough to recognize the complexity of such systems. For example, platforms are typically funded via advertising, and any transparency requirement should cover both organic and paid content. Second, social media platforms allow numerous types of content to be exchanged, and one-size-fits-all approaches to the kind of metadata that must be made available are unworkable. Instead, the kind of data required to be released must be tailored to the particular type of content. Ads, pages, shared URLs (Uniform Resource Locators), and so forth all have different types of metadata that need to be shared. Third, transparency over who sees the content is crucial to understand platforms' impact. While existing data have focused primarily on the content itself, making aggregate data on the demographics of who is being shown the content is equally as important, as it's necessary to be able to understand the platforms' impact on end users.

In summary, social media platforms do not currently have the proper incentives to allow research on their platforms, and have been observed to be actively hostile to important ethical research that is in the public interest. At the same time that platforms' power and influence is reaching new heights, our ability, as independent researchers, to understand the impacts that they are having is being reduced each day. We need Congress's help to enable researchers to have sufficient access to data and social media platforms in order to ensure that the benefits of these platforms do not come at a cost that is too high for society to bear. Thank you again, and I look forward to your questions.

[The prepared statement of Dr. Mislove follows:]

Written Testimony of Alan Mislove
Professor and Interim Dean
Khoury College of Computer Sciences, Northeastern University

Before the
United States House Committee on Science, Space, and Technology
Subcommittee on Investigations & Oversight

Hearing entitled
The Disinformation Black Box: Researching Social Media Data

Tuesday, September 28, 2021
via Zoom

Chairman Foster, Ranking Member Obernolte, and distinguished members of the Subcommittee, thank you for the opportunity to appear before you today to discuss accessing and analyzing data from social media companies.

My name is Alan Mislove. I am a Professor and Interim Dean of the Khoury College of Computer Sciences at Northeastern University. My research is on *algorithmic auditing*; I develop methodologies that allow me to study large online platforms—such as those operated by social media companies—to better understand how they work, how they may be abused, and what impacts they are having on end users. I conduct my research independently: Without companies' permission, and without insider access to data. Put simply, I have no more access to these platforms than any of you do. This is a significant challenge: It is difficult to develop the techniques that enable my work, especially because companies are resistant to external accountability and we work in a legal environment makes such research carry non-trivial risk.[1]

With that context, as Congress is considering legislation in this area, I am well-positioned to provide input on what currently can be measured about social media platforms, and what is needed going forward to ensure researchers fully understand the impact that these platforms are having on society at large. In particular, there are four messages I wanted to convey in response to the questions the subcommittee posed:

1. Independent research is *critical* to uncovering and addressing platforms' societal impact

Today, social media platforms mediate an increasingly large fraction of online communication, ranging from interpersonal communication to political messaging, from news dissemination to access to life opportunities. Even in the best of worlds, understanding how these platforms are impacting end users and society is too big a task for the platforms themselves. In reality, despite the critical role they play in our society, social media platforms are frequently non-transparent about the content that is shared on their platforms, as well as the advertising systems that fund their operations.

Despite these challenges, my group and collaborators have been successful at studying a variety of such platforms, identifying alarming behaviors, and working with platforms to make improvements. We

[1] *Sandvig v. Sessions — Challenge To CFAA Prohibition On Uncovering Racial Discrimination Online.* https://www.aclu.org/cases/sandvig-v-sessions-challenge-cfaa-prohibition-uncovering-racial-discrimination-online.

have shown how popular e-commerce platforms often use techniques such as price discrimination to maximize profit at users' expense[2]; how online "gig economy" hiring platforms can rank candidates in ways that disadvantage women[3]; how ride-sharing services were calculating "surge" prices[4] and how they are impacting legacy taxi services[5]; and how social media platforms' algorithms can produce large distortions in the racial and gender makeup of who sees ads, often without the advertiser's input or even awareness.[6] In the coarse of doing this research, we identified bugs in Uber's surge pricing algorithm[4] and privately disclosed to Facebook multiple ways in which malicious advertisers could leak private user data.[7] In both cases, the platforms fixed the issues we identified.

The upshot is that independent, third-party research is critical to fully understand how social media platforms are impacting end users and society as a whole.

2. Today, independent researchers' access to data is *woefully* inadequate

Today, the kinds of questions that researchers are able investigate are severely hampered by researchers' limited access to platforms, as well as the platforms' choices about what to make available. Typically, studies are based on running experiments directly on the platform and collecting data, on recruiting cohorts of real users who agree to share their data, or on analyzing the aggregate data that the platforms provide.

When we run our own experiments, because every platform is different, we must typically spend significant time to understand what kind of data we can get out of the platform, and whether that data is useful scientifically. For example, when studying Facebook's advertising platform, we ran our own ads and measured how they are being delivered using Facebook's interface that tells advertisers how their ads are performing. For our experiments alone, we spent over a year understanding how the ad platform can be used to measure the properties of the underlying relevance algorithm, and spent over $25,000 actually running ads.

This approach to studying platforms requires deep computing expertise to develop, is expensive in both money and time, and is not scalable to address the impact that platforms are having. Worse, the answers we can find with it and conclusions we can draw are often relatively small in scope, relative to the impact that platforms are having on society. For example, we can often only comment on how *our own content* is treated, making it difficult to understand what is happening to others'. This means we can often show that the ad platforms' algorithms have certain properties, but it is much more challenging to understand the degree to which those properties impact real-world ads and end users.

When we recruit cohorts of real users, we often ask users to install software such as browser extensions or mobile applications in order to collect data automatically. These users are typically compensated, and

[2]Aniko Hannak et al. "Measuring Price Discrimination And Steering On E-commerce Web Sites". In: *ACM Internet Measurement Conference*. Vancouver, Canada, Nov. 2014.

[3]Aniko Hannak et al. "Bias In Online Freelance Marketplaces: Evidence From Taskrabbit And Fiverr". In: *ACM Conference on Computer Supported Cooperative Work*. Portland, Oregon, USA, Feb. 2017.

[4]Le Chen, Alan Mislove, and Christo Wilson. "Peeking Beneath The Hood Of Uber". In: *ACM Internet Measurement Conference*. Tokyo, Japan, Oct. 2015.

[5]Shan Jiang et al. "On Ridesharing Competition And Accessibility: Evidence From Uber, Lyft, And Taxi". In: *International World Wide Web Conference*. Lyon, France, Apr. 2018.

[6]Muhammad Ali et al. "Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead To Biased Outcomes". In: *ACM Conference on Computer Supported Cooperative Work*. Austin, Texas, USA, Nov. 2019.

[7]Giridhari Venkatadri et al. "Privacy Risks With Facebook's PII-based Targeting: Auditing A Data Broker's Advertising Interface". In: *IEEE Symposium on Security and Privacy*. San Francisco, California, USA, May 2018.

we go to great lengths to ensure that they understand the experiment and that their privacy is protected. However, this methodological approach has a number of drawbacks: it is difficult to recruit a diverse and representative population of users, it is expensive to do so at large scale, it is technically challenging to collect data when users are on mobile devices, and platforms often use technical and legal means to attempt to prevent data collection in this manner despite these projects having user consent.[8,9,10]

When we rely on the aggregate data that platforms themselves provide, researchers face challenges of first obtaining access to the data (which is not always possible), determining whether the data is scientifically useful, and putting faith in platforms that the aggregation was done correctly. For example, Facebook's Ad Library ostensibly shows, for political ads, "a range of how much they spent, and the reach of the ad across multiple demographics".[11] However, this data is limited in significant ways: the amount spent on an individual ad is provided only in coarse-grained ranges, the demographic breakdown of who actually saw ads is provided only at a superficial level, and no targeting information is revealed. The situation is worse for non-political ads, where none of this information is available at all. Similarly, Facebook's Open Research and Transparency (FORT) initiative provides targeting information for political ads from a particular three-month period, but omits information on ads with fewer than 100 impressions[12] (likely a large fraction of the ads during that period, making it difficult if not impossible to answer most scientific questions). Worse, this data set is not public, requires approval from Facebook to be able to access, and cannot be shared with other reseachers.

When relying on platform-provided aggregate data, researchers must further trust that the platform correctly aggregated the data. This trust may be misplaced, as evidenced by a recent incident in which Facebook's data provided to the Social Science One initiative left out data from *half* of U.S. users[13], calling many previously-published studies that relied on the data into question. Finally, platforms have often under-invested in even the simple data transparency tools they do provide. For example, the Facebook Ad Library has been shown to have numerous reliability issues[14] that has made it difficult to use it as a basis for scientific work. Similarly, another popular data tool, CrowdTangle, is reportedly in the process of being broken up by Facebook.[15]

3. Major platforms are actively attacking independent researchers' ability to do their work

Researchers today are effectively relying on platforms' "good will" to allow studies to be run at all—a situation that is becoming less and less tenable as platforms become more entrenched. In some cases, platforms refuse to many available data that would enable necessary research. To wit, Facebook recently criticized[16] a study on misinformation by saying it focused on who engages with content and not who sees

[8] *Facebook Seeks Shutdown of NYU Research Project Into Political Ad Targeting.* https://www.wsj.com/articles/facebook-seeks-shutdown-of-nyu-research-project-into-political-ad-targeting-11603488533.

[9] Engadget. *Researchers shut down Instagram study following backlash from Facebook.* https://www.engadget.com/algorithmwatch-facebook-shutdown-184729493.html.

[10] The Markup. *Facebook Rolls Out News Feed Change That Blocks Watchdogs from Gathering Data.* https://themarkup.org/citizen-browser/2021/09/21/facebook-rolls-out-news-feed-change-that-blocks-watchdogs-from-gathering-data.

[11] *What is the Facebook Ad Library and how do I search it?* https://www.facebook.com/help/259468828226154?helpref=search.

[12] *Facebook Open Research & Transparency.* https://fort.fb.com.

[13] The Washington Post. *Facebook made big mistake in data it provided to researchers, undermining academic work.* https://www.washingtonpost.com/technology/2021/09/10/facebook-error-data-social-scientists/.

[14] The New York Times. *Ad Tool Facebook Built to Fight Disinformation Doesn't Work as Advertised.* https://www.nytimes.com/2019/07/25/technology/facebook-ad-library.html.

[15] The New York Times. *Inside Facebook's Data Wars.* https://www.nytimes.com/2021/07/14/technology/facebook-data.html.

[16] The Washington Post. *Misinformation on Facebook got six times more clicks than factual news during the 2020 election, study says.* https://www.washingtonpost.com/technology/2021/09/03/facebook-misinformation-nyu-study/.

it—but that's only true because Facebook does not make such impression data available to researchers. While research may sometimes be going on inside companies—where researchers presumably do have access to such data—public relations concerns are paramount and can prevent important findings from being shared. For example, Facebook reportedly recently blocked the publication of a report[17] that indicated the top-performing story on their platform was, in fact, COVID-19 misinformation.

In other cases, social media platforms are actively hostile to third-party research, and sometimes even going as far as blocking researchers and threatening legal action. For example, just in the past few weeks we have observed Facebook block the accounts of New York University researchers[8] and threaten the European group Algorithm Watch[9] with litigation, both for running independent, ethical research in the public interest.

4. Mandating transparency requires nuance, but is feasible and urgent

Social media platforms sit inside broader social-technical systems, and the data made available to researchers must be comprehensive enough to recognize the complexity of such systems. However, addressing these challenges is feasible, and is becoming increasingly urgent.

To understand why comprehensive data is needed, consider the recent debate over ad *targeting options*, which can enable advertisers to limited their ads shown to heavily biased—and potentially discriminatory—groups of users. One might think limiting advertisers' ability to use various targeting options would address this concern; however, our work has demonstrated that doing so can actually cause ads to be shown *more* biased groups. The reason is that not all users targeted by the advertiser actually see the ad: Platforms typically have *relevance algorithms* that select the subset of the targeted users to whom content is most relevant. Thus, by removing targeting options, the relevance algorithms tend to have greater leeway in choosing which users actually see the ad as the targeted groups tend to be larger.[18] In this example, for researchers and policy to fully understand the impact of relevance algorithms—as well as to develop effective policy mitigations—platforms need to provide data on *both* the ad's targeted audience as well as the actual delivery audience.

Different kinds of content require different kinds of data. It is important to note that social media platforms typically allow sharing of a variety of different types of content. For example, Facebook alone allows "organic" posts (which can contain mixes of text, images, videos, etc); aggregate content including pages, events, and groups (themselves containing users, posts, and other data); ads (each containing creative content, targeting information, external links); and many others. Because each kind of content has different features and attributes, a one-size-fits-all approach to making data available is unworkable. Instead, when platforms are required to make data available, the kind of data that is released should be tailored to the particular type of content.

Transparency over both "what" and "who" is crucial to understand platforms' impact. Specifically, existing platform-provided transparency mechanisms have focused primarily on making data available on the (popular) content that is being shared, while there has been much less emphasis on data about *who* this content is being shown to. Making aggregate data on the demographics of who is being shown

[17] The Washington Post. *Facebook says post that cast doubt on covid-19 vaccine was most popular on the platform from January through March.* `https://www.washingtonpost.com/technology/2021/08/21/facebook-coronavirus-vaccine/`.

[18] For example, when we targeted an ad for jobs in the janitorial industry to an equally gender- and race-balanced audience on Facebook, it was delivered disproportionately to Black women (compared to jobs in the lumber industry, which were delivered disproportionately to white men).

content is critically important, as it is necessary to be able to understand platforms' impact on end users. Unfortunately, without the requirement to do so, platforms have been resistant to releasing such data: for political ads only, Facebook reveals demographic breakdowns for only the users who saw the ad, whereas Google reveals demographic breakdowns for only the targeted users.

Finally, while ethical concerns exist over social media platform data, these have successfully been addressed historically, and existing approaches could be used directly when sharing this information. Moreover, scientific communities are used to addressing the ethical implications of scientific research, and have processes in place to ensure protection of human subjects and that research meets community ethical standards.

To conclude, social media platforms do not currently have the proper incentives to allow research on their platforms, and have been observed to be actively hostile to important, ethical research that is in the public interest. At the same time that such platforms' power and influence is reaching new heights, our ability as independent researchers to understand the impact that they are having is being reduced each day. Thus, I and other researchers need Congress's help to enable researchers to have sufficient access to data from social media platforms in order to ensure that the benefits of these platforms do not come at a cost that is too high for society to bear. In particular, proposed legislation such as the Algorithmic Justice and Online Platform Transparency Act of 2021 and the Social Media Disclosure And Transparency of Advertisements (DATA) Act of 2021 both take meaningful steps towards ensuring researchers continue to have sufficient access to such data.

Thank you again for giving me the opportunity to appear before you at today's hearing. I look forward to your questions.

Alan Mislove is a professor, the senior associate dean for academic affairs, the associate dean for faculty affairs, and the interim dean at the Khoury College of Computer Sciences at Northeastern University. He received his bachelor's, master's, and doctorate in computer science from Rice University in 2002, 2005, and 2009, respectively. After receiving his doctorate, he joined Northeastern's teaching faculty as an assistant professor of computer science.

Mislove's primary field of interest concerns distributed systems and networks, with a focus on using social networks to enhance the security, privacy, and efficiency of newly emerging systems. He is a core faculty member of the Cybersecurity and Privacy Institute, which forages partnerships with experts in the industry, government, and academia worldwide.

In 2019, Mislove won the IRTF Applied Networking Research Prize for IMC '17 paper for his work on understanding the role of registrars in DNSSEC deployment. His work has been funded by Amazon Web Services, the Army Research Office, the Data Transparency Lab, Facebook, Google, and the NSF. He was a recipient of the NSF Career Award in 2011, and his work has been covered by *The Wall Street Journal*, *The New York Times*, and CBS Evening News

Chairman FOSTER. Thank you. And next is Ms. Edelson.

TESTIMONY OF MS. LAURA EDELSON,
PH.D. CANDIDATE AND CO-DIRECTOR
OF CYBERSECURITY FOR DEMOCRACY
AT NEW YORK UNIVERSITY

Ms. EDELSON. Good afternoon—good morning, Chairman Foster, Chairwoman Johnson, Ranking Member Obernolte, and the Members of the Subcommittee. My name is Laura Edelson. I'm a Ph.D. candidate in Computer Science, where I also co-lead the Cybersecurity for Democracy Project, and I'm a Belfer Fellow with the Anti-Defamation League. As cybersecurity researchers, my team and I study systemic vulnerabilities in online platforms that expose people to misleading and false claims, from fake COVID cures, to voting disinformation, to investment scams, primarily on Facebook. Our ultimate goal is to develop workable solutions to digital mis- and disinformation. Members of this Committee will understand that in order to do this we need concrete data, and the ability to engage in rigorous scientific inquiry of that data. And lack of data is currently the most serious barrier to the work of misinformation researchers. Twitter is the only major social media platform that allows most researchers access to public data on their platform, albeit at a high financial cost.

In 2016 Facebook got a—bought a company called CrowdTangle that offered access to public Facebook data, and it still operates their offering. However, very few researchers are allowed to access this tool. It's primarily offered as a business intelligence product. Most other platforms, including YouTube and TikTok, simply offer nothing. In the face of this black box, some researchers, including my team, Mozilla, and news outlets like The Markup, have attempted to crowdsource data about what happens on social media. We have been met in some cases with outright hostility from the platforms we study. This summer, after months of legal threats, Facebook cutoff my team's access to their data. We are far from the only research team that's been stopped. Algorithm Watch in Germany was forced to shutter their work entirely after Facebook threatened legal action against them. Many other researchers who would like to study at this—study Facebook at this point are frozen out. They simply can't afford a legal battle with one of the most powerful corporations in the world.

We had used the data we got from Facebook to support the finding in our most recent study that posts from disinformation sources got six times more engagement than that of factual news, to identify security vulnerabilities that we reported to Facebook, and to monitor Facebook's own public-facing ad library for political ads. Every day that my team can't access the data we need to do our work puts us further behind in a race to find answers. And make no mistake, the harm being caused by misinformation and hate online is very real.

In 2019 journalist Jeremy Merrill reported that conservative retirees were targeted with misleading claims in Facebook ads, and then guided to sites to convince them to trade in their retirement funds for precious metals with a company called metals.com. In the summer of 2020, an advertiser on Facebook called Protect My Vote

ran ads discrediting mail-in balloting that were aimed at African-American voters in the Upper Midwest. A report from the Anti-Defamation League found that exposure to videos from extremist or white supremacist channels on YouTube remains common, with one in 10 study participants being exposed. And nearly 40 percent of Latinx respondents said that they'd seen material that makes them think that the COVID vaccine is not safe or effective, according to a study earlier this year.

But I know I don't need to remind any of you who experienced the invasion of the Capitol on January 6 of the high costs of misinformation to our social fabric. Facebook particularly is a selective megaphone. Their own internal research has shown that the way they have built their algorithm disproportionately promotes misinformation and extreme content. To study these issues, all researchers need access to much more data than Facebook or most other platforms provide. Facebook should strengthen CrowdTangle by adding data about user platforms, and broaden access to it so that researchers from all institutions can use it. Other companies, like Google and TikTok, should make public data about their platforms accessible to researchers as soon as possible.

Facebook needs to reinstate my team's accounts immediately so that we can resume our work. And while we hope this will happen soon, we must also acknowledge the platform's attempts at voluntary transparency have failed. It's time for Congress to act to ensure that researchers and the public have access to data that we need to protect ourselves from online misinformation. I believe we will look back and see this moment in history as a turning point when the costs of disinformation and hate online became too great to ignore, and we stepped up and took action.

Previous generations of Americans have taken on public health crises like cancer or drunk driving, and science has helped us to meet tough challenges like this, and this helped us to save lives, and to make the lives we save more enjoyable and fulfilling. Science can help us now, but only if we provide researchers the data that we need to study and describe the problems we face. In closing, I want to thank the Committee for their attention to these issues, and also for the opportunity to share my experience and perspective.

[The prepared statement of Ms. Edelson follows:]

Testimony of Laura Edelson, NYU Cybersecurity for Democracy

Before the
Subcommittee on Investigations and Oversight
U.S. House Science, Space, and Technology Committee

Hearing on "The Disinformation Black Box: Researching Social Media Data"

September 28, 2021

Good afternoon Chairman Foster, Ranking Member Obernolte, and the members of the subcommittee. I am extremely grateful for the committee's attention to the harms being caused by misinformation on social media, and the difficulties researchers face in trying to study this threat to public health, safety, and our democracy.

My name is Laura Edelson, and I am a Ph.D. candidate in Computer Science at New York University. I also co-lead the Cybersecurity for Democracy project at NYU's Center for Cybersecurity, and I am an ADL Belfer Fellow. As cybersecurity and privacy researchers, my colleagues and I at NYU study systemic vulnerabilities in online platforms that expose people to misleading and outright false claims – from fake Covid-19 cures, to voting disinformation, to investment scams. I believe we will look back and see this moment in history as a turning point, when we stepped up as a society and took action to address what is now a pervasive problem. Previous generations of Americans have taken on similar social ills such as smoking, drunk driving, and industrial pollution. Revelations from investigations by the Wall Street Journal and The New York Times over the past week show that Facebook has internal research demonstrating specific harms and differential treatment and on its platforms, and has considered certain mitigation strategies, only to discard them. These findings which have now been made public echo the conclusions of both my work and the work of other independent researchers: Facebook amplifies misinformation and extreme content. Facebook's most influential and powerful users are often the ones spreading the most far-reaching misinformation because Facebook doesn't apply its own policies and rules evenly. Facebook can be harmful to the mental health of its users.

Clearly, we can't rely on the platforms alone to reduce these harms on their own. Members of this committee will understand that we need to base solutions on independent, rigorous, scientific inquiry based on concrete data. Unfortunately, researchers have been severely hampered not just by lack of such data, but also outright hostility from platforms toward our research. Indeed, this summer, Facebook cut off my team's access to their data. We used that very data to support the finding in our recent study that posts from misinformation sources on Facebook got six times more engagement than factual news during the 2020 elections, to identify multiple security and privacy vulnerabilities that we have reported to Facebook, and to audit Facebook's own, public-facing Ad Library for political ads.

Every day that my team cannot access the data needed to do their research puts us further behind in the race to find answers. Meanwhile, mis- and disinformation continues to contribute to real world harms. Facebook needs to reinstate our accounts immediately so that we can resume our vital work. While we hope that Facebook will do this soon, we must also acknowledge that the platform's voluntary transparency efforts have failed. It's time for Congress to act to ensure that researchers, journalists, and the public have access to the data we need to both study online misinformation and build real solutions.

The Social Media Black Box

Currently, researchers have only limited access to social media data, even when that data is technically public on the platform. Though there are some avenues for study, they fall far short of what is necessary. We really are faced with a black box when it comes to understanding how information flows on these platforms.

Twitter sells access to a small percentage of public tweet data via an interface called the Firehose API. This tool was designed for business use, but researchers who can afford to pay for access to it have used it to study the spread of disinformation and hate on Twitter. Because of its high cost, however, it is out of reach for many researchers based at universities and non-profit organizations. Nonetheless, it represents the most comprehensive dataset that a large platform has allowed researchers to access.

Facebook makes some public Facebook and Instagram content available via its CrowdTangle platform. CrowdTangle was originally developed, and is still primarily marketed, as a business analytics tool that major Facebook accounts can use to understand how well their content performs on the platform. More recently, Facebook has offered CrowdTangle to researchers and journalists, and the tool does contain vital information for those tracking and studying misinformation on the platform. However, Facebook severely limits journalists' and researchers' access to CrowdTangle. In the past month, I have heard from researchers across a wide range of institutions who have been unable to secure access to this source of data; in fact, the tool seems to be out of reach for the majority of the disinformation research community. Additionally, Facebook maintains an online ad library. However, researchers and developers may access the Ad Library API only if they sign an agreement that limits how they use and share the data, which significantly hampers meaningful publication of any research findings, as the dataset that would be necessary for other researchers to reproduce any findings cannot be publicly shared. Meanwhile, Facebook has shown itself willing (as in my case) to cut off access to the API when it threatens to produce research that is inconvenient or embarrassing to the platform. And the data it does provide is often unreliable. In recent weeks, both the New York Times and Politico have reported on separate major data errors in Facebook's transparency tools for researchers that were discovered by academics attempting to use those tools to audit the company's claims.

Other platforms offer even less information. For example, Google has no comparable program to Facebook's for researcher access to public YouTube data. It does publish transparency

reports with extremely limited data about electioneering ads in the U.S. I consider Google to be the least transparent of the major social media platforms. Finally, most smaller social media platforms, such as TikTok, have no mechanism of any kind for researcher access to either public user generated content or ads.

Many of the transparency efforts that do exist, even for public data, are so access-limited that other researchers cannot reproduce studies that rely on that data. This cuts off a vital part of the scientific process and hamstrings scientific research into what happens online. Lastly, the data that is available via existing transparency efforts are so incomplete that their usefulness for research is needlessly limited. For example, Facebook doesn't make information about how many users have seen a piece of content available through CrowdTangle, even though they could easily do so, and having access to this user impression data would help us better understand why misinformation sometimes spreads so quickly.

As is obvious by now, these avenues for study are grossly insufficient to inform and meet the needs of the public and researchers. In the face of these serious deficiencies, journalists and academics have developed some independent data collection efforts. For example, because the initial focus of my research was focused on the role that advertising plays in disinformation and discrimination online, my team developed Ad Observer, a browser extension that allows users to voluntarily – and anonymously – share information about the ads that Facebook and YouTube show them. Crucially, the tool collects information about the way each ad was targeted by the advertiser. This information – which might reveal, for example, that an advertiser targeted "married men" or "African-American culture – helps us understand how advertisers exploit Facebook's micro-targeting tools, often to spread disinformation and to single out groups they believe will be particularly receptive to it. The Ad Observer tool does not collect personally identifying information, both because that would not meet our ethical standards and because we don't need to do so to answer our scientific questions.

Ad Observer has yielded information we could not get if we relied on Facebook alone. For example, thanks to our 16,000 volunteers, we've been able to collect data from Ad Observer that demonstrates that the archive of political ads Facebook makes available to researchers is missing more than 100,000 ads. Using Ad Observer data, we have also discovered that there are several categories of political ads that Facebook has deliberately and categorically excluded from its political ad archive — such as ads purchased by organizations that Facebook determines to be "news publishers," and posts that advertisers pay social media influencers to promote.

In addition to my team's project, there are a small number of other research efforts. One notable example is the Markup's Citizen Browser project. This project, in a little over a year, has uncovered how Facebook continues to allow advertisers to target users by race via proxy interests even after it said it would end the practice, how it continues to recommend anti-vaccine groups, and how it continues to allow financial products to be targeted by age.

One of the reasons there are so few of these projects is because of the legal threats that platforms – and Facebook in particular – have made against independent researchers. Last October, for example, Facebook sent me and my colleague, Professor Damon McCoy, a letter claiming that Ad Observer violated Facebook's terms of service. Facebook demanded that we deactivate the tool and delete the data that our volunteers had donated for study. Shortly after, your colleagues on the Energy & Commerce committee sent Facebook a letter highlighting both the safety and importance of our work, and encouraging the company to work with us to allow the continued operation of our tool. Regardless, on August 3, after months of negotiations over Facebook's demand, the company suspended our Facebook accounts. Although the suspension of our accounts has not affected the Ad Observer tool, it has effectively terminated our access to Facebook's Ad Library API and to CrowdTangle. We relied heavily on both the Ad Library and CrowdTangle in our research. Other researchers and journalists have received similar threats from Facebook.

While these independent data collection projects are needed, they are not enough on their own to provide the information that we need about the platforms. There are vital holes in our understanding that we simply can't fill without additional data. The most serious limitation that researchers face today is that there are many platforms, such as YouTube and TikTok, that do not provide even limited researcher access to data. The Mozilla Foundation has published crowdsourced reports illustrating problems such as political influencers evading a ban on political ads on TikTok, and users' stories of YouTube algorithmic recommendations promoting misinformation. We need more data from these platforms to dig more deeply into these concerns.

What Researchers Need, and Why – a Better Black Box

After a plane crash, NTSB investigators seek access to the flight data recorders – the black box. This allows them to analyze what happened so future disasters can be avoided and culpability can be determined. Social media platforms control the equivalent of the black box of data about online misinformation that could help researchers analyze how it contributes to violent events such as the January 6 attack on the Capitol.

There is a great deal of public data on social media platforms, most notably ads, that can and should be made publicly available in a machine-readable format for the use of researchers and journalists from all types of institutions. Last year, I led a public call for Universal Ad Digital Transparency. I believe this proposal should be implemented by all major digital ad platforms immediately. Real harm is still being done by misinformation in digital ads:

- In the summer of 2020, an advertiser called "Protect My Vote" ran ads discrediting mail-in balloting that appeared to be aimed at African-American voters in the upper Midwest.
- Conservative retirees were targeted with misleading and out-of-context claims in Facebook ads, then guided to sites to convince them to trade in their retirement funds for

precious metals with a company called Metals.com, according to reporting by journalist Jeremy Merrill for Quartz in 2019.
- While Facebook announced it would remove racial categories as a way advertisers could target ads, The MarkUp's Citizen Browser project reported that proxy categories were still in use–examples include "African- American history," "Hip hop music," "Latino music," and "National Hispanic Heritage Month."

We also need broader access to public, non-paid content on social media platforms. Right now, this could be done by broadening access to platforms like CrowdTangle, and by Google allowing researchers more access to public YouTube data. We know there is harm being done by the rampant spread of misinformation, hate, and misrepresentation online, even if we don't yet know the full extent of the problem.

- Our forthcoming study shows that, across the political spectrum, posts from news sources that regularly traffic in misinformation have a statistically significant and large engagement advantage–by a factor of six—over posts from news sources that have a record of factualness.
- People who rely on Facebook for information have substantially lower vaccination rates than those who rely on other sources, according to a survey conducted by the COVID States project in June/July 2021. Of those who rely exclusively on Facebook for news, 25 percent say they do not intend to get vaccinated. This is not an issue of partisanship: both the vaccination odds and the vaccination rates for people who get their news exclusively from Facebook are lower even than for those who get their information exclusively from Fox News.
- A report from the Anti-Defamation League found that exposure to videos from extremist or white supremacist channels on YouTube remains common, with one in ten study participants being exposed to such content.
- In March 2020, Facebook and Twitter announced that they removed a network of Russian-backed accounts, originating in Ghana and Nigeria, that targeted Black communities in the U.S. Similar to voter suppression campaigns in 2016, the accounts appeared to be operated by people in the U.S. and attempted to build an audience by posting about Black history, Black excellence and police brutality.
- Nearly 40 percent of Latinx respondents said they've seen material or information that makes them think the COVID-19 vaccine is not safe or effective, according to a survey earlier this year by Change Research on behalf of the Latino Anti-Disinformation Lab. Another 20 percent said they have directly received wrong or harmful information about the vaccine, primarily on Facebook (53%).

Ad Observer: Why and How we Protect User Privacy

Protecting user privacy is crucial, and Congress and the public are rightly concerned about it. But the good news is we don't need – and definitely don't want– to expose people's private information in order to study misinformation and share our findings with the public. Lung cancer researchers don't publish the names of individual smokers, and we don't need to reveal

identities and people's online browsing habits to expose the systemic vulnerabilities leading to the spread of misinformation.

We believe Facebook exploited concerns about user privacy as a pretext to squelch our research and use us as an example to chill other researchers in our field when they cut off my team's access to data. Our Ad Observer tool does not collect data about our volunteers or their friends. Ad Observer does collect the names and Facebook pages of paying advertisers – examples might be ExxonMobil, Biden for President, The Daily Wire, or the Democratic Underground. What we've learned is that when Facebook said we were violating user privacy, they were talking about advertisers -- not users like you and me. And as Facebook itself makes clear, all Facebook ads are public information.

In their blog post defending cutting off our access to data, Facebook attempted to lay the blame for their own actions at the feet of the FTC by citing the 2011 consent order they signed. We were extremely grateful when, two days later, Sam Levine, Acting Director of the Consumer Protection Bureau issued a letter clarifying that the FTC consent order does not, in fact, bar Facebook from creating exceptions for good-faith research (like ours) that is in the public interest. Despite this, Facebook has still not restored our accounts.

We go to great lengths to ensure that our tool does not collect personal information about the users who install it, or their friends. Ad Observer has been vetted by Mozilla's security engineers, who found no privacy concerns. And of course, all of our research protocols are regularly reviewed by NYU's Institutional Review Board, which oversees all our work. Ad Observer meets the highest standards of user privacy and ethical research. Facebook hasn't acted against us because our project is a threat to its users, but because they perceive our research as a threat to themselves and their bottom line. They are attempting to silence science when our findings are inconvenient, and their message to other academics is clear: criticize us at your peril.

Congress must take action to ensure data access needed to study misinformation

After having now spent several years researching this field, I believe that it is time to acknowledge that voluntary transparency has failed. It has failed to protect consumers from dangerous disinformation, failed to provide scientific researchers with sufficient data to make constructive recommendations to the platforms and the public, and failed to be a trusted source to inform users about their practices and consequences. These transparency schemes that platforms have put in place as a stop-gap measure until Congress is able to act are falling prey to many of the common pitfalls of voluntary regulation. Facebook in particular has changed its rules for what it makes "transparent" multiple times, and now it wields its API agreements like a weapon, threatening academics and journalists whose research it doesn't like with the threat it will cut them off from data necessary for their work.

First, Congress should pass a law requiring Universal Digital Ad Transparency now. The biggest digital ad platforms should be required to make all the ads they run publicly available in a machine-readable format. Along with nearly a dozen researchers, I called for universal digital ad transparency last year. We will soon be publishing a draft proposal that spells out the technical specifications needed in detail.

Second, I believe that a researcher safe harbor law would help protect the many researchers who engage in direct collection of data from platforms. The passage of this law would not directly give researchers access to data, but it would clarify the legality of a great deal of work that currently exists in limbo.

Third, platforms should be required to make public data available to the public: that is, public content with meaningful reach or content from public figures with meaningful audiences should be made available to researchers via tools or searchable interfaces that are accessible to researchers and journalists for analysis. Posting on public pages is analogous to slapping up a notice on a town bulletin board, or writing a letter to the editor. The intended audience is: everybody. Researchers should be able to collect this information for analysis.

Conclusion

In closing, I want to thank the committee for the opportunity to share my experience and perspective. When I began studying for my Ph.D. I did not expect the road I was on would lead here. But I believe that more data and the scientific process is exactly what we need to meet this moment in history, as we grapple with unforeseen consequences of new technologies. Science has helped us meet tough challenges before, helped us save lives and make the lives we save more enjoyable and fulfilling. Science can help us now, but only if we provide researchers the data they need to study and describe the problems we face. Your attention to this topic is vital if we are to make progress, and I know I'm not alone among my colleagues in offering whatever help I can provide. Thank you.

###

Laura Edelson is a Ph.D. Candidate in Computer Science at NYU's Tandon School of Engineering. Laura studies online political communication and develops methods to identify inauthentic content and activity. Her research has powered reporting on social media ad spending in the New York Times, the Wall Street Journal and the Atlantic. Prior to her current time in academia, Laura was a software engineer for Palantir and Factset. During her time in industry, her work focused on applied machine learning and big data.

Chairman FOSTER. Thank you. And after Ms. Edelson is Dr. Leicht.

TESTIMONY OF DR. KEVIN LEICHT, PROFESSOR, UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN DEPARTMENT OF SOCIOLOGY

Dr. LEICHT. Yes, thank you, and thank you for—to the Committee for inviting me. My name's Kevin Leicht. I'm a Professor of Sociology at the University of Illinois Champaign-Urbana, and I have assembled a multi-disciplinary team that is studying how misinformation spreads through social media platforms, and what effect labeling has on dampening the spread of that misinformation. What my group of social scientists, computer scientists, and journalists, and business professors has found is that consistent labeling by social media platforms about COVID–19 severity, transmission, vaccinations, and cures is somewhat effective at preventing the spread of social—suspect social media posts. But because of Facebooks algorithms, and their lack of access to them, we can't really tell whether reduced sharing of suspect posts is due to Facebook's algorithm or changes in actual user behavior, and this unsatisfying outcome is probably why I was invited to speak to you today.

Though we know quite a bit about how misinformation spreads, so we know it's not necessarily spread by nefarious individuals on the dark web, and we know what types of people are susceptible to consuming this information, we also know that combatting this information is harder the more misinformation is repeated, so it becomes harder and harder to stop. But, as our prior two testifiers have said, social media platforms keep their data to themselves, and they discuss—do research internally that is not disclosed. The platforms do offer places to download such data, but much of the research happens in lab settings where researchers tightly control what people see, which is not—which is valuable, but is not really what happens in the real world of social media consumption.

With the black box algorithms that social media platforms use, users get vastly different exposures to different types of informations—different types of information, and we are left studying what users do with bits of information without knowing exactly what the stimulus is that's prompting them to share this misinformation. There are deficiencies in the tools needed to do this research, the data availability, which has already been discussed, and there's an overall lack of coordination in the study of social media information and data collection.

The data availability part, as our prior presenters have said, is important for independent research. The simple answer to this problem, when I talk to outsiders, is I say this. We didn't trust The Tobacco Institute to tell us about the safety of smoking. We probably shouldn't rely on social media companies for research on what social media does. That research needs to be done independently. They have a built-in conflict of interest with regard to this research, as their purpose is to draw attention and eyes, and the information that draws attention and eyes sells advertising. The biggest gap that we see in doing research is in the data and algorithms, or the black box the social media companies use to deter-

mine what end users see. And at some level we need access not only to the data, but to the black box.

There are some things the Federal Government can do, I think, to help social media researchers, and allow independent social media research to be done, which I think is vitally important. The strategy my group thinks of would combine action by the Federal Government to compel the social media companies to share data, contributions by the social media providers themselves, help from private foundations, and help from private Federal science funders. The Federal Government could require the platforms to provide data to research groups who are investigating public interest questions about misinformation incidents, prevalence, and consequences, and this data sharing could take many forms.

There could be central—we could see the creations, for example, of central data depositories like we have in astronomy, for example, or in other social science areas, where there are depositories that act as a basic infrastructure for studying social media information, so people don't have to reinvent the wheel every time they want to study social media information, collect their own misinformation, deal with—or deal with the possible legal consequences, and everything else. And the access to this data could be through some sort of cloud computing format, with strict human subjects protocols, so many more researchers would have access, and they wouldn't have to jump through the hoops that our group has had to jump through here. And with that, I'll conclude my remarks. Thank you.

[The prepared statement of Dr. Leicht follows:]

THE DISINFORMATION BLACK BOX: RESEARCHING SOCIAL MEDIA DATA

Testimony before the

House Science, Space and Technology Committee

Subcommittee on Investigations and Oversight

September 14th, 2021, 2 PM (EST)

Kevin T. Leicht

Professor of Sociology

University of Illinois Urbana-Champaign

Thank you for the opportunity to present our thoughts on social media data, social media misinformation, and the promises and pitfalls of researching social media data in our current economic and political landscape. I have spent most of the 1990s and 2000s studying the political and social consequences of social inequality and cultural fragmentation. Much of this work has focused on the changing landscape and growing skepticism confronting experts in most scientific fields. Much of this new skepticism is shared and spread via social media and attacks established, scientific knowledge across the board.

In my recent and on-going research (with colleagues Joseph Y. Yun, Geis College of Business, University of Illinois, Brant Houston, John and James L. Knight Foundation Professor of Investigative Journalism at the University of Illinois, Loretta Auvil, Senior Project Director at the National Center of Supercomputing Applications, University of Illinois, Peter Ondish, Research Scientist at the Center for Social and Behavioral Sciences, University of Illinois, Peter Evans, Professor of Sociology and Director of the Computational Social Science Program at the University of Chicago, and Prassana Balprakash, Senior Project Director, Argonne National Laboratory), I have examined how misinformation spreads via social media and whether

attempts by social media platforms to label such information has been effective in reducing sharing practices by users.

Our preliminary findings suggest that reliable and consistent labelling of social media misinformation by Facebook regarding COVID-19 severity, means of transmission, efficacy of vaccines, and potential miracle cures has been somewhat effective at preventing the spread of suspect posts. We have also discovered that Twitter does relatively little labelling of any kind, which is contrary to what we believed was their stated practice. However, because of the way Facebook's algorithms work, and our general lack of access to them as researchers, we are not able to tell whether the reduction in sharing of posts labelled as misinformation results from changes in algorithms (where posts labelled as misinformation are less likely to be prominently placed, less likely to be seen by end users, and thus less likely to be shared), or whether the reduction in sharing is due to actual changes in user's sharing behavior.

This unsatisfying outcome of our research so far highlights some of the problems I will highlight as I answer the committee's questions. While my research group has been helpful in constructing these answers, this testimony should be viewed as mine alone.

1. What patterns have you observed in how misinformation and disinformation spreads on social media platforms and the effectiveness of platforms' moderation techniques?

Apart from our research, there is quite a lot of research investigating how social media misinformation spreads, along with methods for debunking or flagging misinformation and mitigating its spread.

The proliferation of misinformation across Facebook and Twitter is generally quite similar and is often coordinated. The same posts or highly similar posts appear in both places. Contrary to what one might think, much of the low-credibility information comes from high-

profile, official, and verified accounts rather than muddy sources on the "dark web" (see Yang et al., 2021). As researchers and experts begin to fight misinformation contained in social media posts, there may be an uptick in creative ways to embed misinformation in new posts (by, for example, embedding texts in photos).

The spread of social media misinformation is also driven by differences in the actual people consuming the information. Personality type often predicts receptivity to misinformation (Axt et al, 2020) as well as demographic factors like age (older individuals tent to be more susceptible) and technological literacy (those will less tech literacy tend to be more susceptible, see Nagler et al., 2019). Laboratory studies suggest that one leading cause of misinformation spread is being overwhelmed with information – people cannot deliberately process and make accurate assessments when there is so much information being conveyed (Pennycook et al. 2020). There is also evidence that misinformation spreads not because it is fake, but because it is attractively packaged and unconstrained by reality (Acerbi, 2019). Laboratory studies also suggest that emphasizing publisher quality (e.g., The New York Times vs. Breirbart) may not reduce susceptibility to social media misinformation either (Dias et al., 2020). Clearly some people are more vulnerable to spreading misinformation than others and the sheer amount of information overwhelms many people.

The pervasiveness of social media misinformation has led to quite a bit of research on ways of combatting it. Repeatedly seeing fake news increases believability, even when the stories are labelled as "disputed", except in extremely false cases (e.g. the Earth is a perfect square, see Pennycook et al., 2019). Flagging suspect social media posts works in many situations but not all of them (Swire-Thompson et al., 2020). More detailed debunking methods work better than cursory methods – citations to more credible information tend to work better

than a simple label (Chan et al., 2017). Finally, there is some evidence that who flags the information and who is debunking it has some effect, especially if the flagging is done by another person or by an AI algorithm (Yaqub et al., 2020.

In summary, we know a few things about misinformation and disinformation spread and some of the attempts to combat it. Despite this research, social media companies keep much of their data internal, so it is challenging to get an accurate assessment of how effective these platforms are at moderating misinformation. The social media platforms conduct many algorithmic and psychological studies internally, but the results are not disclosed. Some social media platforms like Facebook and Twitter do offer places where researchers can download data about posts and tweets (e.g., the CrowdTangle API for Facebook) and one can get an idea about the prevalence of certain types of posts through these tools. But most of the research that attempts to understand the causes and consequences of social media misinformation use lab settings that are much more controlled and very different from where users see misinformation as consumers. In lab settings, we can control the treatment that people are exposed to and then see what they do with that information. However, the black box algorithms the social media platforms have means that end users are exposed to vastly different "treatments" and we are left trying to understand what they do with the information without knowing what the initial stimulus was.

2. What are the limitations of current tools, techniques and data sets used to analyze social media?

There are serious limitations to the current tools and data sets available to analyze social media data. Those limitations fall into three general categories: (1) limited tools, (2) limited data availability, and (3) lack of coordination.

First, there are a limited number of tools available that are a combination of free/low cost and accessible to those that are not computer scientists. I believe we all can recognize that it's important to allow non-computer scientists to analyze social media at a relatively low cost, but such tools are few and far between. Some examples of tools that help in this way are NodeXL, Gephi, SNAP, and Professor Joseph Yun's own open-source tool, the Social Media Macroscope (at the University of Illinois). We need more funding to continue to build these tools to expand the number of researchers who can conduct this valuable work.

Second, there are limited amounts of social media data available due to company restrictions placed on that data. Many researchers fear litigation that may result from analyzing and publishing results from these data.

Third, there is little coordination regarding the analysis of social media data, especially for the sake of national security and societal wellbeing. Our group has advocated for the creation of national think tanks or laboratories to study social media effects on culture, social cohesion, and political life. In effect, each new researcher confronts the social media landscape virtually alone and without a lot of infrastructural help or assistance.

3. What kind of data can and should be made available by social media companies in order to understand the spread of misinformation and disinformation and its impact on society? Why is it important that researchers independent of social media companies have access to social media data?

A good start regarding data availability would be to focus on the data surrounding media platform misinformation and filtering. At present, this type of data and the algorithms used are less than transparent. There would need to be an open and ongoing conversation between social media companies and the research community, preferably a community represented by centralized think tank(s) for national social media research.

This access needs to be independent from the social media companies themselves because they have a conflict of interest with regards to researching and policing their own content. The goal of the social media companies is attention and engagement and, if extreme content produces that attention and engagement, that means more profit. Pursuing profit is not wrong, but one could question whether this model is contrary to overall social well-being.

The same holds true for research investigating misinformation on social media sites where social media platforms have a potential conflict of interest as well. This conflict of interest is most apparent in 1) the types of research questions investigated by social media companies from the onset, 2) how they interpret and understand the results they obtain, 3) how they report those results to public stakeholders (e.g., individuals, government, etc.), and 4) any action social media companies may or may not take based on their findings. This problem is compounded by the general lack of sharing of research results by the social media platforms.

4. How can the Federal government assist researchers in accessing data from social media companies that can help shed light on the spread of misinformation and disinformation?

Ideally the Federal government should work in concert with social media companies, private foundations, and Federal science funders to craft policies that require social media platforms to provide data for third-party groups to investigate specific, public-interest questions about misinformation incidence, prevalence, and consequences. This type of research would allow for independent checks and research on the power and impact social media companies have on misinformation and its spread.

The ways this data could be made available for researchers to use could take many forms. The creation of central data depositories of the kind that support other sorts of science infrastructure (for example, the Interuniversity Consortium of Political and Social Research, a

data depository at the University of Michigan) might be one model. Access to social media posts, platform algorithms, and sharing patterns could be provided to researchers who meet relatively strict human subjects/data confidentiality protocols. Another possibility would be to make social media platform data available in a restricted use data context, much as individual Census records are protected via Census Data Use Centers on university campuses. Other models are possible via cloud computing applications and depositories whose access could be relatively open while adhering to prevailing data confidentiality protocols.

This kind of policy would be another concrete step by the Federal government to formally consider misinformation for what it is: a public health and national security issue. To date, the deliberate spread of misinformation online has disrupted the US's efforts to address climate change, has enabled terrorist recruiting and communication, has eroded trust in political leaders, and continues to thwart efforts to vaccinate populations against COVID-19. More generally, misinformation threatens to untether the US population from reality by undermining our ability to preserve and recall a collective human history. Solving these public health, national security, and existential threats to the nation will require shared data and effort among industry, academic, and government partners.

Kevin T. Leicht is Professor and former Head of the Sociology Department at the University of Illinois at Urbana-Champaign and former Chair of the Department of Sociology and Director of the Iowa Social Science Research Center at The University of Iowa and past Program Officer for the Sociology and Resource Implementations for Data Intensive Research Program at the National Science Foundation. He is the past editor of *Research in Social Stratification and Mobility* (the official journal of the Social Stratification Section of the International Sociological Association) and *The Sociological Quarterly* (the official journal of the Midwest Sociological Society).

He has written extensively on issues relating to economic development, globalization, and political sociology, his work has been funded by the National Science Foundation, National Institutes of Health, Spencer Foundation, and the Ford Foundation, and his published articles have appeared in the *American Sociological Review*, *American Journal of Sociology*, the *Academy of Management Journal*, *Law and Society Review*, and other outlets.

He is the author or editor of five books including *Professional Work* (with Mary Fennell, published by Blackwell), and *Postindustrial Peasants: The Illusion of Middle-Class Prosperity* (with Scott Fitzgerald) winner of the Midwest Sociological Society Best Book Award for 2009, and *Middle Class Meltdown in America* (2014, also with Scott Fitzgerald). His current research examines the consequences of extreme inequality in developed societies and the social and cultural consequences of male marginalization.

Chairman FOSTER. Well, thank you. And at this point we will begin our first round of questions. The Chair will now recognize himself for five minutes.

I'd like to start out my questions by entering a statement for the record prepared by the Center for Countering Digital Hate, which studies how dangerous content spreads online and harms society at large, whether it be offensive hate speech, or misinformation aimed to change people's beliefs and behaviors for the worst. So I'd ask unanimous consent for that statement to be entered into the record. Hearing none, so ordered. And now on to my questions.

Dr. Mislove, in your research you have purchased ads on Facebook, and used the performance metrics to gain insight into the algorithm that determines who actually sees the ads. You noted in your testimony that your team has spent over $25,000 running ads. Frankly, it strikes me odd that researchers are in the position of having to pay the subject of their study in order to gain sufficient access to crucial data. But—so, first, how do the metrics available to you as a paying advertiser differ from those that are available to researchers who are not paying for privileged access, or what forced you to go and decide to spend money here?

Dr. MISLOVE. So thank you for the question, Chairman Foster. You're precisely right, we have used the advertising system as a methodology. The reason is that if you are not using that, and using the publicly facing data, the most useful thing is what's called the ad library. Laura alluded to that. That only gives extremely coarse-grained statistics on active ads. You can't look back, you get no idea of the breakdown of who's actually seeing the ad, their gender, and the delivery location.

When you become an advertiser, you get access to much more fine-grained data. For every ad you run, Facebook gives you very detailed information about how much money is being spent on that ad, the demographic makeup of who is being shown it, and that is what we use as the basis of understanding the delivery algorithm itself. In other words, the decisions that Facebook is making about which users get to see which ads.

Chairman FOSTER. Yes. You—do you ever worry that Facebook knows who you are, and might sort of give you a warped view of the way they treat advertisers?

Dr. MISLOVE. That's a fantastic question, and we do. We actually sometimes use multiple accounts, some of which don't reveal to Facebook, to make sure that our—we're seeing consistent behavior across those accounts. But yes, we do worry——

Chairman FOSTER. You worry about it, OK.

Dr. MISLOVE. We do worry about it.

Chairman FOSTER [continuing]. The ridesharing companies a while ago, you know, got caught doing things like that.

Dr. MISLOVE. Precisely.

Chairman FOSTER. Is there an ethical or privacy-related reason to share more data with paying advertisers than researchers?

Dr. MISLOVE. There's no user privacy related reason to do so. The statistics we get back do not tell us anything about the actual people who see our ads. Again, it's just fraction of men, fraction of women. Facebook will claim that there is, and I think Laura may

have some words about that, but that—when they say that, they're protecting the privacy of advertisers, not the privacy of end users.

Chairman FOSTER. OK. Is there an agreed-upon list that's—about what sort of information, you know, that is available to advertisers now that should just be—automatically be available to researchers? Would that be a reasonable, you know, mandate for social media generally?

Dr. MISLOVE. I don't know that such a list exists right now, but it would not be difficult to develop exactly such a list. There are big—they already release certain metrics, and I would argue that there are a number of others that we already have access to in various ways that could become the basis of such a list.

Chairman FOSTER. Yes. Dr. Edelson, in your testimony you mentioned CrowdTangle and Twitter's Firehose API (application programming interface) being primarily business analytic tools. Are—so are businesses getting access to information that researchers aren't when these tools are being, you know, throttled, or not made available to researchers? And how does their intent—their design intent, as business analytic tools, limit their usefulness to researchers?

Ms. EDELSON. Thank you for the question. So, in short, yes. We've found CrowdTangle to be quite a rich tool for studying user engagement, and it was quite illuminating for that purpose. But as researchers, you know, we don't just want to be able to, you know, come to this conclusion, misinformation is very engaging. We would also like to be able to understand—to start to be able to understand how we could stop that, how we could design systems to make misinformation maybe less engaging. And in order to do that, one of the things that we really need is impression data. This is something that would be really, really crucial to actually start getting to solutions, and it's something that Facebook doesn't make available through CrowdTangle.

If I could just speak very quickly to the prior question about ad data? I actually published—I have a pre-print of a paper that's available that has a—that is a technical standard for what data could be made available about ads. I'd be happy to forward that on to you. It's going to be published in the next couple of months formally.

Chairman FOSTER. Thank you, I appreciate that. And I'll now recognize Ranking Member Obernolte for five minutes.

Mr. OBERNOLTE. Thank you very much, and thank you to our witnesses. It's been a very interesting hearing. Let me start with Ms. Edelson. You had something in your written testimony that you didn't have time to bring up in your oral testimony, in which you made some recommendations about things that can be done to facilitate access to information, and one of the things that you proposed was to create a legal safe harbor for researchers in working with this data. And I wanted to give you a platform to elaborate a little bit on that, but if you could also, as you talk about that, if you could talk about whether or not that legal safe harbor should also apply to the platforms themselves, since, ostensibly, they would be giving you that data that create liability for them as well?

Ms. EDELSON. Thank you for the question. I think it's a very good one. So the researcher safe harbor proposal that the Knight

First Amendment Group and I have called for would provide legal protections to researchers like me who engage in direct study of platforms by using it. I think that's the general thrust. There are many excellent researchers who do really important ethnographic work, I'm thinking particularly of Joan Donovan out of Harvard, who does really good work studying militia groups, how they recruit, other extremist groups like this, and this would provide cover to these researchers for their work so that—you know, again, within bounds, that they handle data responsibly, that their work is overseen by institutional review boards (IRBs), that is within ethical boundaries.

As to whether platforms themselves would need legal cover, I think in general I would need to go back and talk to the lawyers about that. To my knowledge, in general, we're covering data that is generally accessible, so I actually don't know if that would be required.

Mr. OBERNOLTE. Interesting. OK. You brought up the institutional review boards, which is something else I have a question about, just because when I got my doctorate, you know, my research was qualitative, and only involved interviews, and yet my IRB gave me a hard time about that data. I can't imagine what yours did to you.

I have a question for Dr. Mislove. In your oral testimony you discussed the fact that running experiments on the platform is beyond the capabilities of a lot of researchers, and yet that seems to be the only way that we can get really unbiased data, because even if we ask the platform owners for data, you know, we have, you know, a concern that the data that we're going to get back is biased in some way, just the same way that if you ask a cigarette manufacturer whether or not tobacco use was safe, you know, you wouldn't necessarily trust the veracity of that data.

I have a further concern about this, though, and—as a computer scientist myself, you know, a lot of these algorithms are interconnected. You know, you can't create a fake user and, you know, run some tests about, you know, what liking this does, or what not liking that does, and to see what kind of—how the algorithm works without affecting real users' pages, right? Because all of that data feeds back into it. So we've kind of got this quantum mechanical situation where the act of observing the system is influencing the behavior of the system. As a researcher, how do you combat that?

Dr. MISLOVE. Those are fantastic questions, thank you for them. So to address your—sort of the first question about sort of the ability to study these, we are able to do it, but the limitation is when we run—when we become an advertiser, we're only really able to say what happens to our own ads, right? So we—it's much harder for us to go beyond that and say, OK, this is the kind of effects we're seeing on other advertisers' ads. So we really can speak to the algorithm a bit, but we can't speak to sort of its impacts on users in many cases.

To your second question around sort of the feedback loops, and these sorts of quantum mechanical effects, as you described them, that's exactly right, and we think very much about that. To give you one example, one of the things we worried about is how much—like, teasing out how much of the effects we see are due to

the users who engage with the content, versus the algorithms that actually, you know, choose who to deliver it to, and Kevin had alluded to that in his testimony.

We have come up with a number of cute tricks to be able to sort of tease those out in many cases, where we can sort of make sure that ads show up as the same to individual users, so we know the users can't react any differently, but the algorithm will see them differently. So there are ways, in certain cases, we can get around that, but it's something we take into account every time.

Mr. OBERNOLTE. Very interesting. Well, Mr. Chair, it looks like the clock is malfunctioning, which I guess is a good thing for me, but I'm just going to ask one final question, and open it up to the whole panel to answer. You know, the end goal here you know, of the research you're doing, I think, is not only to understand how misinformation spreads, but to enable us to reach some kind of societal solution to halting the spread of misinformation without suppressing free speech.

And I think we can get there, right? We've done that in other venues. You can't yell fire in a crowded theatre. You know, that's not—recognized as something that's not infringement on people's free speech because of its potential to cause harm. And I think we're going to reach some kind of standard with that as pertains to online misinformation. And I think, just like we did there, it's going to revolve around the intent of the poster of that misinformation. But I'm wondering if you could weigh in, and anyone would like to, about what you think that ultimate solution is going to look like.

Dr. LEICHT. Can I take a stab at that one? One of the things my group thinks about in that regard, about how to balance the relationship between controlling misinformation and censorship, is to think about simply coming up with more effective labels. So people can post and basically spread anything that they want, so the communication itself is not censored, but one of the things that stops misinformation from spreading as often, the cognitive interference of actually labeling this and say, are you sure you want to spread this or not? But I actually think even something like that is going to have to be fairly conservative, so there will be some types misinformation that are simply not in the public interest to control, or necessarily stop the spread of, and others that's more vital for, say, the public health, or the public safety. So that would sort of be my group's way of dealing with this conundrum.

Mr. OBERNOLTE. Ms. Edelson, go ahead.

Ms. EDELSON. So one of my very recent studies, one of our key findings was that misinformation outperformed factual content on Facebook. But the real meat of this was this was true for every partisan category, so far right misinformation outperforms far right factual content. Far left misinformation outperforms far left factual content. So I think we all want to get to a place where misinformation isn't prioritized, it is not in a fast lane against factual content, and we can do this without discriminating based on viewpoint, or suppressing—you know, suppressing certain opinions, or certainly suppressing facts, as you've spoken to. I think what we need to get to is a place where engagement—user—you know, user interactions is not the driving force of what content is promoted.

Mr. OBERNOLTE. Right. OK. Well, thank you very much. It's been really interesting. I look forward to the rest of the questions. Despite what's on the clock, I'm sure I'm out of time, so, Mr. Chair, I'll yield back.

Chairman FOSTER. Thank you. And I guess, if there's Member interest, we can certainly entertain a second round of questions here, because this is—I can't imagine a more important subject, actually, right now. And so I'll now recognize my colleague from Illinois, Mr. Casten, for five minutes.

Mr. CASTEN. Thank you, Mr. Chairman, and thanks to our witnesses here. This is really fascinating. The—about three years ago, relevant that this was before COVID, and I feel somewhat prescient in an angry way, Mark Zuckerberg testified before Financial Services Committee, and I asked him in the first instance whether they would suppress anti-vaccine information if it came from Jenny McCarthy's Facebook page, and then separately whether they would suggest—suppress information from the American Nazi Party if it came from Art Jones's Facebook page. Art Jones, at the time, had just won the Republican nomination to run for Congress in Illinois's 3d congressional District. His answers were unsatisfactory, and seemed to suggest that the content of the information was one question, the speaker was another.

I mention that because the recent *Wall Street Journal* reporting that they are, in fact, whitelisting certain high-profile people suggests that this problem has not been solved. And I'd like to start just with Ms. Edelson, because it sounds like you've spent a lot of time thinking about this. Do you see a disparate approach to information protocols depending on the speaker in your research as we sit right now? Sorry, I think you're muted.

Ms. EDELSON. There certainly currently exists, you know, as we all now know, two separate systems on Facebook, where some speakers are effectively not moderated at all, and then there's everyone else. I think this is almost entirely backwards, because what Facebook has set up is a situation where these speakers who have the widest reach are free to spread, you know, whatever lies they choose, and it will take a long time for Facebook to act, and often Facebook won't act at all.

I think that we do—that—you know, this is where I think there is a difference in how we think about content moderation versus how we think about content promotion. I think that speakers that have a bigger audience should have a bigger responsibility to ensure that the information that the platforms spread on their behalf to their audiences is factual.

Mr. CASTEN. Yes. That—I think we're all fond of the framing that freedom of speech and freedom of reach are two separate things, and I think sometimes we allow them to amplify horrible messages that would go away if we just limited it to freedom of speech.

My next question, I want to start with Mr. Mislove, but I—if we have time, I'd love all of your thoughts on this. I totally agree with your idea that we should have this data shared and available for research. At the same time, there's an implicit premise behind that that says that the data we provide on social media platforms does not belong to us, and the custodian of that data is now the firm

that has the data. And the—I personally have been rather persuaded by Roger McNamee in his writing, that if we gave—if we essentially made sure that everybody is the custodian of your own data, and all of your own metadata, and all of that data was portable, we would essentially end up with a much healthier social media environment because the—essentially there wouldn't be this walled garden, and the conflict of interest where the company that has information about where you traveled last week, who you were with, what you bought, had that information to share.

And I realize that's a long list, and gets a little bit beyond the purview of this Committee, but if we were to wave a wand tomorrow and change the premise such that everybody owned their own data, that they could opt into sharing that data, and the metadata around their data, so that they truly had portability so that they could still say, I actually find it useful that this device knows where I am, and where I want to go, and can have all the automated—if we were to do all that, does that change the environment that you would have where essentially we would have to get sort of permission for the data from the public, rather from the companies, that we have, without really questioning, assume that they're the custodians of the data? So, Mr. Mislove, start with you, because I see you're nodding your head so vigorously, but I welcome all of your thoughts on that question.

Dr. MISLOVE. That's a great question. I'm sure my other panelists will have similar thoughts. So one is that—what you're talking about is essentially sort of democratizing the ownership of data, which there have been a number of proposals to do in—at least in the computer science research literature. It—you know, those sorts of things have some technical challenges, but I think those are solvable. But I think one way you could move toward that is give users legal rights over the data to—that these companies already have on them. So, for example, Facebook allows you to extract your data from the site, but there's many things they don't provide you. We have some information on that. And this—if you allowed users to have the legal right to say, give me all of your data on me, that would enable many more research studies, because you could then get users to contribute their data themselves, with consent and so forth. So the—you know, do—what you're saying, I think there's a number of different ways to tackle it, but it would make significant progress toward enabling researchers to be able to study these systems.

Mr. CASTEN. And I realize we're out of time, and we may come back, but I would be curious if that changes, because now every individual user would have to consent to sharing the data with you to do their research, as opposed to saying to Facebook, just give me the data.

Dr. MISLOVE. Absolutely. It—I mean, in some ways it would make it more challenging, but at the same time we've done those sorts of studies. Like, we've recruited users of—you know, Laura has a whole study where she did exactly that. So there—you know, there's precedent for doing it, and it's something we're used to doing.

Mr. CASTEN. OK. Well, I'm out of time. I yield back. Thank you.

Chairman FOSTER. Thank you. I'll now recognize my colleague from Colorado, Mr. Perlmutter, for five minutes.

Mr. PERLMUTTER. Thank you, Mr. Chair. A couple comments, and then some questions. So one, I have to applaud our Ranking Member, and our Chair, and to the panel, it is the Science Committee, and between the two of them, they are able to weave in quantum mechanics, and usually the Theory of Relativity, into every panel. So—and I just—I want to congratulate the Ranking Member on getting quantum mechanics into this panel. So—No. 1.

No. 2, to the Ranking Member—and, you know, I guess the concern I have, and the general concern that you've raised about misinformation and censorship, I think in this day and age I'm very concerned about The Big Lie, about Joseph Goebbels, and the ability to promote, and promulgate, and propagate The Big Lie. And—so I'll start with you, Ms. Edelson. And, you know, obviously the Anti-Defamation League is something always concerned about the truth. So you said in your op-ed in the *Times*, "In the course of our overall research, we've been able to demonstrate that extreme, unreliable news sources get more engagement, user interaction on Facebook, at the expense of accurate posts and reporting. What's more, our work shows that the archive of political ads that Facebook makes available to researchers is missing more than 100,000 ads." Can you elaborate on those two sentences, first about—you know, and you've talked about it a little bit, but how do you know that this misinformation really is able to spread farther and faster than accurate stuff? You're muted.

Ms. EDELSON. So the way that we know that is we use Facebook's own tools. We use Facebook's own business intelligence tools for understanding how content spreads, how it engages, because that is very much what Facebook wants its users to do. It wants its user to create content, to create—as engaging content as possible, because that is Facebook's business model. It is a user engagement maximization engine, and then it sells that engagement to advertisers. So we used those tools to study, you know, what Facebook told us their users interacted with the most, and that is what we found.

I want to be clear about one thing. I don't think Facebook chooses to promote—it has not sat down and made the choice, we will promote misinformation. What it has done is it has chosen to promote the most engaging content. And when its own internal research told it that the most engaging content was misinformation, it was the most polarizing content, it was hateful content, it didn't do anything about it. It was a conscious choice not to take steps that would increase the quality of its information ecosystem, but would also decrease engagement. And the reason why is ads. Ads are Facebook's business, and, you know, one of the reasons that that finding, you know, that finding that there are many, many, many ads and advertisers who slip through the cracks is that Facebook isn't willing to make its ad platform more secure, more trustworthy, because that would make its ad experience worse, and it would cost it money.

Mr. PERLMUTTER. So let me just stop you because I've got all scientists on here, or engineers, except I'm the lawyer, and at some point it moves from unintentional to intentional. And—so that

would be my argument. And so I want to turn to Professor Leicht for a second. So—and a number of you brought up, you know, would you trust the information that you might get from The Tobacco Institute. And here—so—now, Ms. Edelson is relying on their tools. I mean, how would you approach this thing? Would it be any different than she has, to try to figure out what's going on here? I mean, she's used their own tools to prove a case against them.

Dr. LEICHT. Yes. Well, I would trust her research in part because the tools are what—the tools are in integral part of their business model. So if the tools don't work somehow, or don't promote more engagement, then the company doesn't make as much money. So unless, through the tools, they are somehow feeding her false information that's specifically bespoke and just sent to her, I would be inclined to trust that. But it is another situation where we are basically trusting them, but on the other hand, some of what she's getting access to is sort of behind the wall, or behind the veil, and so—and it's tied to how they make money, so I tend to trust that.

Mr. PERLMUTTER. Thank you. I yield back, Mr. Chair.

Chairman FOSTER. All right. And I guess we now have time for a second round of questions, so I will recognize myself for five minutes.

The first question—you know, how do you publish information here, where the tools that you use are likely to be altered or abolished underneath, you know, your feet? And so, you know, scientific reproducibility, it's the touchstone of everything, seems to be hard to get to. And some of you touched on that in your testimony. I'm just wondering what—the conflicts you see there, and reasonable solutions to them. I think any one of you, just——

Dr. MISLOVE. Just to clarify, did you mean that—how do we study this system when it's changing constantly, and it—you know, our access could be revoked at any moment?

Chairman FOSTER. Correct. And that the access may not be granted to someone who wants to reproduce your results.

Dr. MISLOVE. Um-hum. Yes. No, that—you're absolutely right, that's a real problem for us. When we act as an advertiser, we keep logs of everything, so we have—we get copies of all of the data on our ads, because, like, our accounts could be shut down at any moment, and as a result, we'd lose access to our scientific data. But it is challenging because there are other, you know, features of the platform that one can only access when one has been in the platform for a long time, and so we have access to some of those. And that would mean that other groups would have significant trouble being able to reproduce our results. That's why I think a more sustainable solution would be one where the platforms are required to make data available, so then the other researchers could analyze that data in a way Professor Leicht talked about, and reproduce any analysis that comes out.

Ms. EDELSON. I just wanted to quickly follow onto Professor Mislove's testimony, because there are also some really perverse incentives here. So, for example, Dr. Mislove is the absolute expert in Facebook—in ad—the Facebook advertiser view, but my team engaged in a little bit of that once ourselves. We found a security vulnerability in the Facebook advertising process. I can't say too much about this, unfortunately, because it is a security vulner-

ability, but we reported it to Facebook, and when we did report that to Facebook, Facebook terminated our advertiser account, so we couldn't continue that work. And that's—I know I'm not the only person that that's happened to.

Chairman FOSTER. Yes. So—some of your work involved basically making a Chrome add-on, and so—Facebook had some bad experience with add-on tools, with Cambridge Analytica and so on, so I can understand how they're a little bit reticent to let people make add-ons of various kinds.

Ms. EDELSON. Actually, this was totally separate from that.

Chairman FOSTER. No, I understand it was a different mechanism, but it's sort of a similar approach, where someone claims to be doing research, and in fact are—is doing something much more nefarious. And so I can—you know, they—it will cost them money to do due diligence on people that claim that they're doing research. And so it—you know, that's—it's just one of the many tensions we're under on this. Do you think the best solution is actually not to have to rely on, you know, essentially spyware that people opt into on their browser, and just say—and just provide, under controlled circumstances, direct access to the huge data base of all user engagement?

Ms. EDELSON. I mean, frankly, yes. I think moving toward a world where platforms do not, you know, do not have the—are not the final authority on who gets to study them, that's probably a much healthier environment. I mean, you know, tobacco companies—I forget who made this analogy earlier, but tobacco companies don't get to decide who does research on smoking, and the idea that social media companies get to decide who studies them is perverse.

Chairman FOSTER. Yes. Dr. Leicht?

Dr. LEICHT. If I could add to that, the way social media dialog is taken hold of in American society, you know, social media posts, and the sharing of, is really a public record of our communication with each other, so it's an awful lot like other forms of public records about communication with each other that we store in places like that Library of Congress, or something. So historians, someday, are going to look back at this era, and they're not going to have a very good perception of what's going on because they're not going to have any access to any of the original social media posts that a lot of our discussions were based on, and that's going to not be a good situation at all.

Chairman FOSTER. Yes. Dr. Mislove?

Dr. MISLOVE. Yes, I'll just add on to that to say that the—it would—to echo Ms. Edelson's point, that the current ways that these platforms make data available often allow you to find the malicious actors on their platforms, for example the purveyors of misinformation, right? But they don't allow you to look at the role that the platform itself plays in amplifying that information. So, specifically, we try to study the algorithm, and the data made available via the ad library and other tools don't allow us to tease out what the algorithm is doing versus the malicious actors. So having a regime where Congress would require all data to be released to be able to be studied would allow us to tease out both the malicious actors, as well as the role of the platform itself.

Chairman FOSTER. Thank you. And my time is now up. I'll recognize Representative Obernolte for five minutes.

Mr. OBERNOLTE. Thank you very much, Chairman Foster. So, you know, for the second round, I'd like to take us, like, up to 30,000 feet. We've been talking about, you know, the specific subject matter of this hearing is how do we eliminate the barriers to data to allow researchers to conduct research into the way that misinformation spreads on social media, right? But the big goal here is to try and figure out how to stop the spread of misinformation, which a lot of people have raised different examples of how it's been destructive over the last couple of years. And I have to say, I am not optimistic about this. I'm a pessimist. Ms. Edelson, you were talking about the fact that maybe Facebook hasn't—has not deliberately chosen to provide misinformation, and I know Congressman Perlmutter was skeptical about that. I'm skeptical too, and I don't think it's ever going to be reasonable to think that the data that you're getting voluntarily out of these platforms is going to be unbiased. I mean, there's too big a commercial incentive there.

So I'd like to talk about the business model. And let me also say that, you know, there's been testimony that perhaps a—some kind of framework around users owning their own personal data would solve this problem, and I have to tell you emphatically, I don't think it will. I was—when I was in the California legislature, I was deeply involved in the drafting of the *California Consumer Privacy Act*, so I know a lot about it, but the problem here is not data, and its connection to users. The problem is that these companies have a business model that's based around user engagement. And, you know, they can't even articulate to you, probably, in some senses, how that works, because if you're—if it's a machine learning kind of thing, that's—the goal of—it has the goal of maximizing user engagement, you know, you might not even know that it's promoting this information because, you know, we don't get that kind of information back out of these algorithms. So I'm very skeptical that this is going to allow us to solve the problem.

And I'm wondering your thoughts on this question. You know, should we be focusing more about—on the model. You know, this model where Facebook and Twitter provide you this service for free, and if you don't know how it's being monetized, if you don't know what the product is then the product is you, right? That's what economists say, and that's what it is. They're selling this user engagement. And the reason why you can't pay a monthly subscription fee to Facebook to avoid their advertising is that people would be horrified if they knew what it would cost you, how much money they're making off of each user. So how—he's the question to you. How do we avoid that? I mean, do we outlaw business models like this? Do we need more transparency? What's the ethical way of dealing with this issue?

Ms. EDELSON. That's a great question, and I think the meat of what you're asking is how much is this a systemic issue? And I think the answer is you're right, there is probably an inherent systemic problem with platforms that—whose business model is built around maximizing user engagement. I think—you know, I hear the tobacco company analogy a lot. I think I personally prefer

maybe a pharmaceutical company analogy, because there are good things that come out of social media too, but there are certainly a lot of problems that can happen.

You know, social media addiction is a very real thing. I think that we may be going toward a world where, you know, we can acknowledge that there are good things about social media, and there are risks, and there are harms, and some of these risks and harms are particularly acute for the youngest users. And I think, in a framework like that, you know, we probably need some regulation for this industry, in the same way that we have regulation for pharmaceutical companies, we have regulation for banks. I think, in Chairman Foster's testimony, he—you know, he spoke about this analogy as well, and I think it's an apt one, you know, where we—I think this is something that's important for society, but we all need much better auditing and transparency of how these platforms function.

Mr. OBERNOLTE. Thank you. Any other thoughts about whether or not we need to focus more around maximizing user engagement as a business model? Dr. Leicht?

Dr. LEICHT. I—that—I wanted to say, another way of attacking the business model, or of making the business model a little bit more benign, might be to allow more competition for social media in the first place. So social media is dominated by a very small number of companies that sort of dominate the entire landscape, and if there were more competition over users themselves, and users' attention, then the abuse of the users could probably be reduced somewhat, or I would think it would be—at least be possible that would happen. So that might be one direction to go as well, if the business model itself can't be directly attacked.

Mr. OBERNOLTE. Sure. I've thought about that too, that maybe—you know, similar to e-mail. You know, when I send you an e-mail, you and I don't both have to be on Gmail for you to read what I'm saying, and so maybe we need to think about social media a different way. When I post something, maybe it goes out to everybody, and it's out there in the metaverse, and, you know, if you choose to look at it on Facebook, that's your choice. But I don't know that that solves the bigger problem.

But—I mean, I really think that we, as a society, need to look at this, and also realize, and this is the reason I'm pessimistic—realize that, because there is such a strong commercial incentive, that no matter what we do, it's going to be an uphill battle. I mean, it's like counterfeit tax stamps on cigarettes, right? The commercial incentive for doing that is so strong that no matter how much resource you devote to enforcement, you're still going to have the problem. And, you know, I think that's the ethical situation we find ourselves in with social media. Anyway, my time's expired. I'd love to continue with the conversation, but thanks, everyone, for being here, and thanks for the fascinating discussion.

Chairman FOSTER. And, in fact, it appears as though there are enough interested Members with questions that I would entertain a third round, so if you want to get your—get with your staff and if you're interested and let me know, and we'll consider that. I will now recognize Representative Casten for five minutes.

Mr. CASTEN. Thank you, pleasure to be back. Professor Leicht, in your testimony you said that the companies have a conflict of interest with regards to researching and policing their own content because the goal of social media companies is attention and engagement, and if extreme content produces that attention and engagement, that means more profit. We saw recently that Facebook's own—I think Facebook's own internal analysis was that the majority of people who join hate groups on Facebook join at the recommendation of a Facebook algorithm. Now, I realize I'm going to ask you speculate a little bit, but, to the extent that engaging with extreme content drives engagement on the site, can one reasonably assume that Facebook and other social media companies, either by individual or algorithmically, know where the extreme content is, know the consequences of the extreme content, and are actively encouraging you to engage with it?

Dr. LEICHT. That is certainly possible. I think they—I think that the truth is, because a lot of the sharing is done by the algorithm itself, much as Representative Obernolte said, they probably don't, you know, personally know that this is happening, but they don't really do anything to stop it. So they certainly—so in that sense, especially in the extremist cases, you could be heading toward a—the situation Representative Perlmutter was talking about, where there's sort of almost active negligence here.

Mr. CASTEN. Yes. And I guess, you know, there's a liability question there, but in a lot of other venues, you know, if I had a high speed trading fund that was actively profiting from, you know, that I was anticipating, you know, I don't know, Russian invasions of Crimea, whether or not I did that or the algorithm did that, I might be concerned about the reputational damage that would come from my fund trading on such information, right? But let me——

Dr. LEICHT. Certainly true, yes.

Mr. CASTEN. Let me then take that to a more specific question, because that's a general question, but let's be very specific. A couple weeks ago we recognized the 20th anniversary of 9/11, and among the things we recognized was the complete heroes on Flight 93 who, in a largely pre-internet era, on a plane, within 10 minutes were able to deduce that there was about to be a terrorist attack on the United States Capitol and got together to stop it. Is it reasonable to assume that in the more recent attack on the U.S. Capitol, given how much was being amplified on Facebook, that a bunch of smart computer nerds at Facebook had knowledge a priori of what was being organized? Because those 40 people on 93 figured it out.

Dr. LEICHT. I think it's possible. It's also possible that nobody at Facebook actually bothered to pay attention to what their algorithms were recommending. So whether there was deliberate promotion or deliberate—or—a better description would be, I suppose, benign neglect of what the algorithm was doing. In either case, there's—there are invidious problems there, you know, whether——

Mr. CASTEN. You know, I guess——

Dr. LEICHT [continuing]. An actual person was involved or not.

Mr. CASTEN. I guess we get into a question—and I see Dr. Mislove and Ms. Edelson raising their hands, so let me just—but I do want to make—just make clear that sometimes we get caught in our own knickers when we say, sure, something is immoral, but it's not illegal, so it must be OK. For my money, if I had the capability to anticipate that there was going to be an attack on the U.S. Capitol and I didn't give a damn, there has to be some responsibility there. Shame on us if it's not illegal, but my goodness, don't look the other way. Ms. Edelson, I know you—I saw you wanting to comment there.

Ms. EDELSON. Yes. I'm sorry, this is really—I worked on Wall Street on 9/11. That's—that was a bad day. That was a really, really bad day. And I remember the morning of January 6 because I told my team that morning that I thought it was going to be a bad day, because this is, you know, this is what I live and breathe. I look at this stuff every day, and it's awful.

I don't know if anyone at Facebook knew it was going to be a bad day. I don't work there. But one of the things we do know is that their internal research has been telling them about the extremist problem for years. They knew that their algorithm was promoting hateful and extremist content. They knew that there were fixes. They knew that those fixes might come at the cost of user engagement, and they chose not to put those fixes into place. So as to whether anyone knew on January 6, I don't know, but they knew about the problem, they knew how to fix it, and they chose not to.

Mr. CASTEN. Thank you. I yield back, unless the Chair would like to allow Dr. Mislove to comment.

Chairman FOSTER. I'll—yes. If you can give a 30 second——

Dr. MISLOVE. I'll just add on that the fact that—like, the—your question goes at the heart of this hearing, which is that we—that—it's a question that we don't know the answer to, and as researchers, as outsiders, we don't have the ability to answer. So that—so, essentially, it's really pointing out exactly why, you know, legislation in this area really is needed. I will say that what we do know is that when we have run political ads, we became a political advertiser and ran that, we do see exactly the echo chambers that you—that could lead to these sorts of things. When we run ads, they deliver more right wing messages toward more right wing users, and vice versa for left wing messages. So we know the algorithm has these effects, and it's incredibly important that we understand how those are playing out in the ways that you're alluding to.

Mr. CASTEN. Thank you. I yield back.

Chairman FOSTER. Thank you. And I'll recognize Mr. Perlmutter for five minutes.

Mr. PERLMUTTER. All right. Well, that exchange was particularly sobering. Sean, nice questions. I think you mentioned one thing about reputational damage, and Professor Leicht, you know, talked about the market control that these companies have. If you're a monopolist, it's hard to have reputational damage. I mean, you've got it. You—you're it. It doesn't matter. There's nobody else to go to. So my question is much more—kind of baseline, for me. In the introduction, I don't know if it was Bill that talked about it, or one of the panelists, talked about sort of the ability to study Twitter

versus the ability to study some of the others, particularly Facebook. Can somebody explain that to me? That it was expensive for Twitter, but at least it was possible. So I just open it to the panelists.

Ms. EDELSON. So Twitter has a—what's called the Firehose API. You can buy access to, you know, all of Twitter—well, a fraction of it, and there are researchers who do this, but it is quite expensive to use. There are also some—Members of this Committee will appreciate the replicability issues that we face, because there are some issues with data portability, but this is why Twitter is the best study platform. Alan?

Dr. MISLOVE. And we have historically gotten access to exactly that Firehose API, which is really useful, and Twitter deserves credit for making that available. I will note, though, that it is an incomplete view. It doesn't cover many of the ad targeting information that we've talked about in this hearing, it doesn't cover delivery information, and so forth. It really lets you get a view of a random fraction of the public content shared on Twitter.

Ms. EDELSON. And then CrowdTangle has a view to public pages and groups on Facebook and Instagram, and there is both a web portal and an API. That's what folks who ingest large volumes of data, such as I used to do, use. And then, for platforms like YouTube, we really don't have anything. There's just—that really is a black box. TikTok is a black box.

Mr. PERLMUTTER. OK. Thank you. I yield back, Mr. Chair.

Chairman FOSTER. Thank you. And it's my——

Mr. PERLMUTTER. And this——

Chairman FOSTER [continuing]. Understanding——

Mr. PERLMUTTER. This has been—I just want to say, this has been fascinating. I've got to leave, but if we have some follow up hearing at some point, I think it would be fantastic. So thanks to the panelists.

Chairman FOSTER. Thank you. And, let's see, I—it's my understanding that Representative Obernolte, and potentially Mr. Casten, are up for another round of questions. Is that—all right, all right, well, then I think that's a quorum for that, and we'll proceed. Let's see.

So when you think about, you know, data portability standards, imagine that you're some startup social media firm. Putting all of this apparatus on top of you is going to be a huge operational cost. And so, you know, it seems likely that we're going to have to make this—OK, until you've got a million users, or something like that, to have a very light touch on this. But at some point we're going to have to scale the mandates here. And—so one way to make that less of a burden is to actually, from the start, have data portability and access standards that they can design their software around, so from the start they can know that when we get big, our data layout and so on is compatible with that. Is that something that's been thought about? And just, you know, any of you can grab onto that.

Ms. EDELSON. So——

Chairman FOSTER. Otherwise there's a danger that we'll just squeeze everyone but the big players out of the business with a bunch of burdensome requirements.

Ms. EDELSON. So I, along with some other researchers at Mozilla and with the Wesleyan Media Project, as I mentioned, we published a technical standard for universal ad transparency. There's a pre-print that's available right now, I'd be happy to send it to you. We will be publishing it more formally soon. When we looked at this issue, what we actually found is that we think it will be less expensive for platforms to comply with just general data access than it would be for them to have to build the large public web portals that companies like Facebook and, to a lesser extent, Google do provide for ads. Because just shipping data is not actually that expensive, as long as there is a standard format that they can comply with.

There's a different question here if we're talking about other forms of non-ad data, organic data, because the volumes of data get really, really large. The recommendation—so I—this is something that I am working on developing a technical standard for. I think our recommendation will likely not require an archive. I think the recommendation that we'll be making in a paper I'm developing is for public access, so we could come to a place where there is programmatic access to the same content that is publicly available, and meet some other thresholds. And that is given, again, to—you know, to researchers who have registered for our program.

And I think, again, as long as there is a standard in place, complying wouldn't be terribly expensive. I do think there is a competitiveness concern, so I do think that probably there's going to be a minimum size threshold that goes into place, but I think you are right that the research community needs to do more here.

Chairman FOSTER. And when you talk about, you know, sort of—people's right to have access to their data, one of the big problems there is that a lot of the data is purchased from third parties, and so what you're going to have to get to is sort of an identifier for people, some unique identifier for people, that they can stand up and say here, you know, this is Bill Foster, you know, here's my—whatever my identifier is, and everyone who has passed around data on me will have a duty to respond to that request. And if they've sold it to someone, or if you purchased it, you're going to have to maintain sort of the chain of custody of who sold the data to who, to who, to who, and keep that identifier around, and keep up a response—you know, a duty to respond to that sort of request, either for access to your own data, or deletion of that data.

And has—have people tried to write down such a system? How that would work, how you'd pretend—how you'd avoid things like identity fraud, and people stealing your entire data set by claiming they were you? Has—have people attempted that sort of—to design systems like that?

Dr. MISLOVE. I can speak a little bit to this, if it—if that was to the panel. The—we've actually done a decent amount of work looking at the data broker industry, which is sort of where these concerns that you're bringing up are sort of the most acute. In fact, many of the data brokers have actually partnered, historically, with social media platforms for the purposes of ad targeting, so that I could target people on Facebook using data-broker derived attributes. And so the upside of all of that is that the—in terms of the unique identifier, they're—the industry is already doing this.

They need to join the Facebook identifiers with the Experian identifiers, and, you know, we know that they're able to do it, even though the information about how exactly they did it is public.

But the—in terms of sort of the identity theft, you know, concerns you raise, that is absolutely a real concern. I will say that there is a little bit of transparency on the data broker industry, that, you know, like, there are certain sites where you can go to see a limited snapshot of your data, and on those sites they have identity verification procedures in place. So I'm not concerned that that's not a solvable problem, that, you know, this has already been solved in other contexts, and so, if there were regulation in this area, I think that would—you know, the technical problems wouldn't be the ones that would come first.

Chairman FOSTER. Thank you. I will now recognize Representative Obernolte for five minutes.

Mr. OBERNOLTE. Thank you, Chairman Foster. Dr. Leicht, if I could ask you about something that was in your written testimony that I found very interesting? You were talking about how research indicates that one of the primary catalysts for the spread of misinformation is our inability as humans to process an overabundance of information. And so I wonder if you could elaborate on that for a minute, and then maybe throw out some possible solutions to that problem?

Dr. LEICHT. Yes. So I—well, unfortunately, that's a problem of the end user. So there's some research that suggests that a lot of misinformation is spread not necessarily because a person is intending to spread misinformation, but because they're bombarded with so much information they're not spending time to cognitively process what they see, so they just forward on posts that look interesting or attractive. And that's—you know, that, I think, is a problem that psychologists have been talking about for years, not only with social media, but in other areas where we're just overloaded with information all the time, and so our ability to process it isn't very good.

One of the solutions to that seems to be to sort of interrupt the automatic process that seems to go on when we read social media sites. So one of the promises of labeling is that—I mean, if you're reading a set of social media posts, and then you come upon something that is labeled, that actually jars you out of this tendency to want to immediately share something gets you to think about whether you want to share it or not, and so it actually slows the process down. And that's a way, then, to get people to think about a specific thing they're reading, and not necessarily this specific thing as one of 200 things I'm reading, and they're all the same. So this is going to be a pervasive problem that is going to be very hard to deal with, but some forms of labeling may help interrupt the process so that just automatic sharing, using essentially our brain stems, is stopped.

Mr. OBERNOLTE. Interesting. So, I mean, what you're talking about is kind of a supply side solution to the problem, where social——

Dr. LEICHT. Yes.

Mr. OBERNOLTE [continuing]. Media companies would be—you know, would be interjecting this in a—you know, in a deliberate ef-

fort to combat the spread of misinformation. But I'm wondering if there might be a demand-side solution. And, Dr. Mislove, maybe I'll ask you about this. You know, is part of the solution perhaps increasing our technological literacy? So, you know, in other words, when—you know, we know that alcohol addiction is a problem in society, right? So we solved that problem, you know, to the extent that we have solved it—we solve it with education, right? If you know you've got alcoholism that runs in your family because they're—the genetic component, you know, if you know that alcoholism can occur, you know, perhaps that you're a little bit more careful about monitoring how many drinks you take, right?

And so I'm wondering if there's—isn't an educational component, like we make people aware of this phenomenon, of how misinformation spreads. You know, we make people aware that you've got confirmation bias, and so that makes you—when you read a piece of misinformation that fits right into your worldview, you're more likely to believe it. You know, and then that way maybe we encourage people to verify the veracity of something before they share it. I mean, is there anything to that, or, you know, or does it have to be a supply side solution?

Dr. MISLOVE. I'll—I think it's a great question. I'll admit it's not my area, so I am truly speculating here, and I'll defer to some of my other—the other panelists to perhaps provide a more detailed answer, but I would think so, and I think—I'll point you to—I know Twitter has recently done a number of things where, if you go to retweet something, but you haven't clicked the link, it will ask you, are you sure you want to do that? Maybe you should read the article first. And so it seems like those are——

Mr. OBERNOLTE. Maybe you should go to Snopes as well.

Dr. MISLOVE. Maybe you should go to Snopes as well. So I think those are inching in the direction of what you're talking about, but some of my—some of the other witnesses may have a more detailed answer.

Mr. OBERNOLTE. Sure. Anyone else?

Ms. EDELSON. The only thing I'll say is that I suspect some kind of demand-side solution, as you refer to it, is going to be necessary, but we don't know what that will look like. It could come in a wide range of forms, and this is actually one of the reasons we need data, because we really do need to start working on solutions, and we need an answer to that question.

Mr. OBERNOLTE. OK. Well, thanks everyone. It's been a really fascinating hearing, and thank you, Mr. Foster, for catalyzing this whole discussion. I've really enjoyed it. I yield back.

Chairman FOSTER. Thank you. And we'll now recognize Representative Casten.

Mr. CASTEN. Thank you, and I echo that this has just been fascinating, and I'm sorry you didn't have the Full Committee, and everybody participating, but I'm actually kind of glad because we've gotten to follow up, and go into a little bit more depth than we usually do.

Ms. Edelson, shortly after you released your results, which found that people who rely on Facebook for information have substantially lower vaccination rates than those who rely on other sources, Facebook cutoff your access to data. I think your research said that

people who rely exclusively on Facebook for news, 25 percent of them do not intend to get vaccinated.

Now, I understand, and I appreciate in your text—I think you said Facebook is using privacy as a pretext to squelch research that it considers inconvenient, and that—I worry sometimes that that sounds like, well, we don't do some research, how much does that really matter? With—I realize we're all math and science nerds here, at least since Mr. Perlmutter has not been able to continue, but at core this is an epidemiological question, right? If we know that certain behaviors increase the rate of spread of a communicable disease, the rate of contraction of communicable disease, there are consequences. And we—you do epidemiology right, people live. You do it wrong, people die. Can you speak at all to the consequences of your inability to do what is at core epidemiological research?

Ms. EDELSON. So I just want to first say the study you're referencing, although it certainly aligns with my work, was done by David Lazer. Excellent work, that I can recommend. But, yes, I think you're right. Misinformation—I'm willing to say this. This misinformation is killing people. We have had a safe and effective vaccine for COVID for a long time now. We're back over 2,000 deaths a day. Facebook is not the only reason this is happening, but it's certainly contributing, because of exactly that study you cite, and that I personally keep in mind.

Right now there is vaccine misinformation that is widespread and easily available on Facebook. I know this because I have colleagues who still do have access to Facebook who find it and try to report it every day. And it's really, really hard for those folks, because they do not feel like the platforms are their allies in this. And, again, this is something that Facebook's own research has pointed to, and Facebook has just chosen not to fix.

Mr. CASTEN. Feel like we're back where we were in the last line of questioning. They know they are causing harm, and choosing not to act. I see a lot of head nods. I'm just getting depressed, so I'm reluctant to ask any more questions. But, Dr. Leicht, Dr. Mislove, anything you'd like to add there?

Dr. MISLOVE. Yes. I mean, I'll just very briefly echo exactly everything Ms. Edelson said, and say that, you know, essentially what you're trying to get at is, you know, how do we fix this? And we've talked to this—in this hearing about a number of, you know, supply side, demand-side, and so forth, but ultimately I feel like, as a scientist, you know, I need to be able to diagnose the problem before I can, you know, understand how to design fixes that will address the problem, and currently we don't have the tools able to do that. We don't know the—you know, how much of the role that the platform is playing, versus the malicious actors that were referred to earlier.

And so I think, for me, you know, sort of going with the phrase, you know, sunlight's the best disinfectant, just being able to understand it can then enable us to develop, you know, mitigations, regulations, whatever it is that would address the issues that we're seeing.

Ms. EDELSON. Just to follow up with that, if the platforms wanted to do one thing today to help start to deal with this problem,

reinstating my account, broadening access to CrowdTangle, would be the most immediate steps they could take, because there are many researchers who want to find answers. They want to be part of the solution, and Facebook is just refusing any help.

Mr. CASTEN. At the risk of being crass, it would seem to be the bare minimum to demonstrate that they give a damn. Thank you all. This has been truly fascinating, and I yield back.

Chairman FOSTER. Thank you, and, before we bring the hearing to a close, I just want to also thank our witnesses for testifying before the Committee today. The record will remain open for two weeks for additional statements from the Members, and for any additional questions the Committee may ask of the witnesses. The witnesses are now formally excused, and the hearing is now adjourned.

[Whereupon, at 11:35 a.m., the Subcommittee was adjourned.]

Appendix

Additional Material for the Record

64

STATEMENT SUBMITTED BY REPRESENTATIVE BILL FOSTER

House Science Committee

Subcommittee on Investigation and Oversight Hearing

on

The Disinformation Black Box: Researching Social Media Data

Statement for the Record

by Imran Ahmed

Founder and CEO of the Center for Countering Digital Hate

Introduction

In the following evidence drawn from the Center for Countering Digital Hate's (CCDH) extensive research of online platforms, we detail the extreme lack of transparency shown by Big Tech and the enormous stakes for society and public health. While conducting numerous independent studies, we have seen up-close Big Tech's stubborn resistance to providing salient information or data access.

Despite our limited access, CCDH reports have demonstrated the enormous reach of online misinformation and documented the resistance of Big Tech to remove dangerous content and users. The Covid pandemic in particular has laid bare the existing real-world harms caused by online misinformation, and the systematic failure of social media platforms to protect their users from those harms. Multiple studies, including our own, have shown that those who are most reliant on social media for information are more vaccine hesitant.[1] Big Tech has proven it is detrimental to public health.

In the last year, we have repeatedly demonstrated that the platforms' systems for preventing the spread of harmful misinformation are not working. The same is true of the systems they have been designed to prevent the spread of hatred such as anti-Black racism, antisemitism and misogyny. Not only do platforms systematically fail to prevent users sharing racist posts, they fail to recognize it and allow such posts to benefit from the algorithmic amplification that social media provides, despite the harm it causes to individual users and to wider society.

---

[1] "The Anti-Vaxx Industry,", Center for Countering Digital Hate, 7 July 2020, page 6, https://www.counterhate.com/anti-vaxx-industry
Lazer, David, Jon Green, Katherine Ognyanova, Matthew Baum, Jennifer Lin, James Druckman, Roy H. Perlis, et al. 2021. "The COVID States Project #57: Social Media News Consumption and COVID-19 Vaccination Rates." OSF Preprints. 27 July 2021. doi:10.31219/osf.io/uvqbs

We also note social media's dominance in the information ecosystem and Facebook's outsized role. We detail the very worrying trends we've observed in how Facebook blocks access to many outside researchers, including restricting access to transparency tools, and the complete inadequacy of Facebook's "transparency" efforts.

We finish by observing that there should be reforms so that the full breadth and scale of Big Tech's harm to society can be assessed. With great power should come accountability and transparency. The Big Tech playbook of deny, deflect and delay, is inimical to the robust and healthy circulation of information in a democracy.

LACK OF TRANSPARENCY: Platforms do not share basic data about what is happening on their platforms

Big Tech platforms are reluctant to share even the most basic facts about the most widely viewed or engaged-posts on their platforms, or about the most influential accounts that they host.

Facebook recently released a "Widely Viewed Content Report" amid reports that its executives were concerned by journalists' attempts to report on the platform's "most engaged with" content using Facebook's own CrowdTangle tool.[2] However, this report carries very little useful information on what content, and particularly what harmful content, users are engaging with on Facebook.

The design of Facebook's new "Widely Viewed Content Report" obscures key facts about the content circulating on the platform, for example by treating links to YouTube as a single category without detailing which videos or channels were most viewed.[3] Its decision to report on views rather than engagement is also puzzling, given that engagement is a better measure of which content users actually pay attention to rather than simply scrolling past in their feeds. Indeed, this is why Facebook has made engagement a key measure of the health of its business.[4]

Similarly, Facebook's transparency reports, intended to detail violations of its community standards, leave simple questions unanswered. These quarterly "Community Standards Enforcement Reports" only tell us the "prevalence" of particular types of violating content, where prevalence is defined as the "estimated percentage of total views that were of violating content."[5]

---

[2] "Widely Viewed Content Report Q2 2021," Facebook, 18 August 2021, https://transparency.fb.com/en-gb/data/widely-viewed-content-report/
"Inside Facebook's Data Wars," New York Times, 14 July 2021, https://www.nytimes.com/2021/07/14/technology/facebook-data.html

[3] "The Most Popular Posts on Facebook are Plagiarized," The Verge, 27 August 2021, https://www.theverge.com/2021/8/27/22644126/the-most-popular-posts-on-facebook-are-plagiarized

[4] "Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead." Wall Street Journal, 15 September 2021, https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215#

[5] "Community Standards Enforcement Report Q2 2021," Facebook, August 2021, https://transparency.fb.com/data/community-standards-enforcement/

As a result, these reports do not tell us the number of times that content was viewed, how much engagement it received or the number of users who were exposed to harmful content, let alone which pages, groups or profiles were most influential in spreading harmful content. The equivalent would be Big Tobacco providing estimated percentages of minors who had succeeded in their attempts to buy cigarettes.

These reports also fail to provide true transparency on Facebook's action against harmful content. They only tell us how many pieces of content resulted in enforcement action, whereas the real measure of the effectiveness of Facebook's reporting systems should be its rate of action against user reports of harmful content that clearly violates its standards.[6]

Transparency reports published by TikTok, Twitter and YouTube suffer from similar limitations.

TikTok's transparency reporting states the number of violating videos that were removed from its platform, broken down by category of harmful content, but does not state how many users viewed or engaged with these videos.[7] It also states the percentage of videos it "flagged and removed automatically" as compared to those removed as a result of user reports, but does not state its rate of action on user reports of harmful content. TikTok does not publish details of the most popular content on its platform, measured either by views or engagement.

Twitter's transparency reporting offers similar details of the number of accounts that were subject to enforcement action, broken down by categories of harmful content, as well as details of how many accounts were reported by users.[8] However, it still fails to report on user exposure to harmful content or its rate of action against user reports. While Twitter does not publish reports on the most viewed or engaged with content on its platform, researchers are able to obtain this information through Twitter's relatively open Application Programming Interface (API).

YouTube reports on the number of videos and comments removed from its platform, broken down by the reason for their removal.[9] However, it fails to detail user exposure to harmful videos except for detailing the percentage of videos that received zero, up to ten, or more than ten views. While YouTube does not officially publish the most viewed videos on its platform for a given period, some insights into popular content are available through its API and third party analytics.

"Report Of The Facebook Data Transparency Advisory Group," Yale Law School, April 2019, page 6, https://law.yale.edu/sites/default/files/area/center/justice/document/dtag_report_5.22.2019.pdf

[6] ibid.

[7] "TikTok Transparency Report," TikTok, 31 March 2021, https://www.tiktok.com/safety/resources/tiktok-transparency-report-2021-h-1?lang=en

[8] "Rules Enforcement 2020 Jul-Dec," Twitter, retrieved 24 September 2021, https://transparency.twitter.com/en/reports/rules-enforcement.html#2020-jul-dec

[9] "YouTube Community Guidelines Enforcement Apr 2021 - Jun 2021," YouTube, retrieved 24 Septemeber 2021, https://transparencyreport.google.com/youtube-policy/removals

All of the above platforms use algorithms to serve users the most engaging content possible, thereby increasing the time users spend on the platform and increasing opportunities to serve them revenue-generating ads. These algorithms determine which content reaches users, in some cases presenting them with content that they have otherwise not subscribed to by liking or following an account.

Despite their fundamental role in serving users content, none of the above platforms publish reports detailing the safety of their algorithms by, for example, measuring how many times the algorithm placed content later identified as harmful into users' feeds.

HARMFUL CONTENT PERSISTS: CCDH investigations reveal platforms are failing to remove content that meets their narrow definitions of unacceptable

Given the lack of useful transparency information provided to researchers by platforms, CCDH has developed methods for externally assessing platforms' reporting systems, algorithms and action against influential spreaders of harmful content.

Platforms often claim that they remove harmful content when it is reported to them by users, but this is simply untrue. Our regular audits of platform action on reports of harmful hate and misinformation show that they fail to act on approximately 8 in 10 posts that violate their standards.

Nowhere has this been more harmful than on their failure to act on reports of clear Covid and vaccine misinformation, as evidenced by three audits of platform action against reports of this misinformation from ordinary users performed by CCDH in the last year.[10]

Our second audit of 912 user reports on Facebook, Instagram, Twitter and YouTube showed that platforms failed to act on 95 percent of Covid and vaccine misinformation.[11] Platforms failed to improve significantly even as social media's role in damaging vaccine confidence became clear. Our most recent audit conducted in March in collaboration with the Canadian Broadcasting Corporation showed that the same platforms were still failing to act on 87.5 percent of user reports.[12]

These failures are primarily a result of platforms' moderation systems. Platform performance in acting on user reports has improved only marginally despite adopting stronger standards on vaccine misinformation.

---

[10] "Will to Act," Center for Countering Digital Hate, 4 June 2020, https://www.counterhate.com/willtoact
"Failure to Act," Center for Countering Digital Hate, 3 September 2020, https://www.counterhate.com/failure-to-act
"Marketplace flagged over 800 social media posts with COVID-19 misinformation. Only a fraction were removed," CBC, 30 March 2021, https://www.cbc.ca/news/marketplace/marketplace-social-media-posts-1.5968539

[11] "Failure to Act," Center for Countering Digital Hate, 3 September 2020, https://www.counterhate.com/failure-to-act

[12] "Marketplace flagged over 800 social media posts with COVID-19 misinformation. Only a fraction were removed," CBC, 30 March 2021, https://www.cbc.ca/news/marketplace/marketplace-social-media-posts-1.5968539

Platforms are no better at addressing user reports of harmful racist hatred. Our recent "Failure to Protect" report showed that Facebook, Instagram, TikTok, Twitter and YouTube fail to act on 84 percent of user reports of clear antisemitic content.[13] Facebook performed worst of all, failing to act on 89.1 percent of reports, despite adopting stronger policies on antisemitic conspiracies and Holocaust denial in the last year.[14]

Last August, as countries around the world entered the second wave of the Covid pandemic, Instagram decided to start placing algorithmically recommended posts at the bottom of users' feeds.[15] This vast extension of its recommendations algorithm, previously limited to the app's "Explore" page, was intended to boost ad revenue by increasing the time users spend on Instagram. However, Instagram did not prevent this feature from promoting harmful hate and misinformation. For instance, our report entitled *Malgorithm* tracked a series of Instagram profiles following the accounts of wellness influencers. These accounts were soon served disinformation from leading online anti-vaxxers "who had been repeatedly flagged to Instagram" in advance of its rollout of this new feature.[16]

In the absence of useful transparency reports about the growth of accounts dedicated to spreading anti-vaccine content, CCDH monitors over 700 such accounts on Facebook, Instagram, TikTok, Twitter and YouTube. This monitoring has revealed dedicated anti-vaxxers across these five platforms are reaching over 59 million followers with harmful vaccine misinformation.[17]

Platforms have also failed to act against the most prolific superspreaders of vaccine misinformation. Our report, *The Disinformation Dozen*, showed that just twelve leading anti-vaxxers are responsible for up to 65 percent of anti-vaccine content. To date, these twelve anti-vaxxers still have 50 accounts across Facebook, Instagram, Twitter and YouTube that reach 7.9 million followers.[18]

BIG TECH'S STRATEGY: Deny, Deflect and Delay

Platforms have denied and, in some cases, directly challenged CCDH for our findings on algorithmic amplification of harmful content and the proliferation of Covid and vaccine misinformation on their sites.

---

[13] "Failure to Protect," Center for Countering Digital Hate, 30 July 2021, https://www.counterhate.com/failuretoprotect
[14] "Failure to Protect," Center for Countering Digital Hate, 30 July 2021, pages 8 and 23, https://www.counterhate.com/failuretoprotect
[15] "Instagram wants you to keep scrolling even longer," CNN, 19 August 2020, https://edition.cnn.com/2020/08/19/tech/instagram-suggested-posts/index.html
[16] "Malgorithm," Center for Countering Digital Hate, 9 March 2021, https://www.counterhate.com/malgorithm
[17] "The Anti-Vaxx Playbook," Center for Countering Digital Hate, 22 December 2020, page 9, https://www.counterhate.com/playbook
[18] "The Disinformation Dozen," Center for Countering Digital Hate, 24 March 2021, https://www.counterhate.com/disinformationdozen

Internal leaks from Facebook to the Wall Street Journal confirm that a small number of "big whales" are responsible for the bulk of anti-vaccine content on the platform.[19] CCDH identified those "big whales" - the Disinformation Dozen - first in March 2021. Our report on the Disinformation Dozen, which analyzed 689,000 pieces of anti-vaccine content posted or shared to Facebook over a period of two months, found that 73% of that content originated from just twelve individuals and their organizations. Between Facebook and Twitter, 65% of anti-vaccine content in our sample was attributable to the Disinformation Dozen.

Mark Zuckerberg was questioned directly about the Disinformation Dozen and the mass of anti-vaccine content on his platforms the day after our report launched in March, when Zuckerberg, Twitter's Jack Dorsey, and Google's Sundar Pichai, testified before the House Energy and Commerce Committee.[20] Twelve state Attorneys General, Senators Amy Klobuchar, Ben Ray Lujan, and the leaders of the House Energy and Commerce Committee wrote to Facebook with concerns about the Disinformation Dozen and Covid-19 misinformation in the following months.[21]

It was not until White House Press Secretary Jen Psaki and President Biden cited the Disinformation Dozen report in July 2021 that Facebook started to take our findings seriously.[22] Monika Bickert, Facebook's Vice President of Content Policy, who herself was questioned by Senator Klobuchar on the Disinformation Dozen in April, penned a blog post disputing our research five months after Facebook was first made aware of it.[23]

Instead of providing the critical data that the White House and independent researchers have long requested, Facebook spokespeople have parroted talking points on tackling vaccine misinformation and refused to disclose the entire universe of Covid-19 and vaccine misinformation -- data they alone are in possession of.

Facebook knew that "big whales" were responsible for spreading anti-vaccine content on their platform. Rather than taking action against these misinformation superspreaders, the

---

[19] Wall Street Journal, 17 September 2021, https://www.wsj.com/articles/facebook-mark-zuckerberg-vaccinated-11631880296

[20] Center for Countering Digital Hate, Twitter, 25 March 2021, https://twitter.com/CCDHate/status/1375134082968006665

[21] Attorney General William Tong letter to tech CEOs, 24 March 2021, https://portal.ct.gov/-/media/AG/Press_Releases/2021/AG-Letter-to-Tech-CEOs.pdf; Senators Amy Klobuchar and Ben Ray Lujan letter to Facebook and Twitter, 27 April 2021, https://www.klobuchar.senate.gov/public/_cache/files/8/7/87e50146-a4cc-4ab1-9604-3190401bbec5/859B41CE812B8AC97F55D24EFEA0F834.4.16.21-letter-to-tech-ceos--vaccine-misinfo-final-.pdf; House Energy and Commerce Committee letter to tech CEOs, 27 May 2021, https://energycommerce.house.gov/newsroom/press-releases/ec-leaders-demand-answers-from-tech-ceos-about-insufficient-progress-to-curb

[22] White House Press Briefing, 16 July 2021, https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/16/press-briefing-by-press-secretary-jen-psaki-july-16-2021/; The Guardian, 17 July 2021, https://www.theguardian.com/world/2021/jul/17/covid-misinformation-conspiracy-theories-ccdh-report

[23] Center for Countering Digital Hate, Twitter, 27 April 2021, https://twitter.com/CCDHate/status/1387086225891340293; "How We're Taking Action Against Vaccine Misinformation Superspreaders," Facebook Blog, 18 August 2021, https://about.fb.com/news/2021/08/taking-action-against-vaccine-misinformation-superspreaders/

company chose to challenge independent research and retain any data that might dispute the publicly available facts.

Anti-vaccine misinformation superspreaders lauded Facebook for this blog post, because they knew that the platform would sooner denounce research into its practices than remove those violating its policies.[24] Joseph Mercola, named by the New York Times as "the most influential spreader of coronavirus misinformation online," has used Facebook's blog to claim he is not an influential spreader of vaccine misinformation.[25] Sayer Ji, another member of the Dozen, claimed that Facebook's blog "validates that there are millions more than 12 standing up to speak out" on Covid vaccines.[26] Ty and Charlene Bollinger, "alternative health" entrepreneurs who are also members of the Dozen, hailed the blog by saying "thank you Facebook for doing the right thing" claiming that the attack on our research "vindicates" them.[27]

FACEBOOK'S UNIQUE ROLE IN AMERICA'S INFORMATION ECOSYSTEM: Facebook is uniquely powerful and has a special responsibility to be transparent

In 1980, nearly seven in ten American adults used cigarettes. In 2021, nearly seven in ten American adults say that they use Facebook and over a third of Americans say it's where they get their news.[28] This shows the vital role of Facebook content in shaping public debate, and places a special responsibility on Facebook to be transparent about the most popular content shaping that debate.

However, Facebook has made it increasingly difficult for researchers to find the most popular content on its platform. It used to be possible to search for Facebook content from particular pages or users, or from particular date ranges, however, these features have been disabled in recent years.[29]

---

[24] "Facebook Vindicates Ty & Charlene and the "Disinfo Dozen"" The Truth About Cancer, 30 August 2021, https://thetruthaboutcancer.com/facebook-vindicates-dinsinformation-dozen/
"Facebook Calls Out CCDH for Manufacturing 'Faulty Narrative'" Mercola.com, https://media.mercola.com/ImageServer/Public/2021/September/PDF/chicago-tribune-misinformation-pdf.pdf
"BREAKING: "Disinformation Dozen": A 'Faulty Narrative' With No Evidence, Says Facebook, Despite 16,000 News Headlines" GreenMedInfo, 19 August 2021, https://www.greenmedinfo.com/blog/breaking-disinformation-dozen-faulty-narrative-no-evidence-says-facebook-despite-1
[25] "Facebook Calls Out CCDH for Manufacturing 'Faulty Narrative'" Mercola.com, https://media.mercola.com/ImageServer/Public/2021/September/PDF/chicago-tribune-misinformation-pdf.pdf
[26] "BREAKING: "Disinformation Dozen": A 'Faulty Narrative' With No Evidence, Says Facebook, Despite 16,000 News Headlines" GreenMedInfo, 19 August 2021, https://www.greenmedinfo.com/blog/breaking-disinformation-dozen-faulty-narrative-no-evidence-says-facebook-despite-1
[27] "Facebook Vindicates Ty & Charlene and the "Disinfo Dozen"" The Truth About Cancer, 30 August 2021, https://thetruthaboutcancer.com/facebook-vindicates-dinsinformation-dozen/
[28] "10 facts about Americans and Facebook," Pew Research Center, 1 June 2021, https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/
[29] "Facebook Quietly Changes Search Tool Used by Investigators, Abused By Companies," Vice, 10 June 2019, https://www.vice.com/en/article/zmpgmx/facebook-stops-graph-search

Now reports have revealed that Facebook is considering closing off researcher access to its CrowdTangle tool, one of the last avenues available for finding the most popular content on the platform.[30]

CrowdTangle has two main functions: a publicly available browser extension and a deeper analytics tool that is only available at Facebook's discretion.

The CrowdTangle browser extension is limited but invaluable, allowing researchers to see how many times a given URL has been liked, shared or commented on across Facebook, and which Pages have shared that URL in posts. We used CrowdTangle in the course of developing our report on the Disinformation Dozen of influential anti-vaxxers to gain a view of how content created by the Dozen had been shared across Facebook.[31]

The full CrowdTangle platform allows users to see what is trending on Facebook in real-time, both across the site as a whole and on specific keywords.[32] However, access to the full CrowdTangle platform is determined solely by Facebook since it purchased the tool in 2016.[33]

This means many researchers are simply refused access to the insights that CrowdTangle could provide. When CCDH inquired about applying for access to CrowdTangle, staff working on the tool refused access, stating that "we've only just started working with a small group of nonprofits."[34] CrowdTangle has been used by nonprofits such as Greenpeace since before its acquisition by Facebook in 2016.[35]

Similarly, Facebook's Ad Library provides welcome transparency but with serious limitations. As has been noted by other researchers, ads only remain in the library's archive if they are concerned with "social issues, elections or politics." Facebook's definition of "social issues" is particularly ill-defined as "sensitive topics that are heavily debated," and this raises questions over whether it should archive a greater range of ads beyond those that it judges to fit this definition.[36]

CONCLUSION: It's Time for Reforms and Accountability

"Facebook is restricting search results – is this taking transparency seriously?" 11 April 2018, https://theconversation.com/facebook-is-restricting-search-results-is-this-taking-transparency-seriously-94762

[30] "Inside Facebook's Data Wars," New York Times, 14 July 2021, https://www.nytimes.com/2021/07/14/technology/facebook-data.html

[31] "The Disinformation Dozen," Center for Countering Digital Hate, 24 March 2021, page 7, https://www.counterhate.com/disinformationdozen

[32] CrowdTangle, retrieved 24 September 2021, https://www.crowdtangle.com/features

[33] "Facebook buys CrowdTangle, the tool publishers use to win the internet," The Verge, 11 November 2016, https://www.theverge.com/2016/11/11/13594338/facebook-acquires-crowdtangle

[34] Email from CrowdTangle to CCDH staff, 16 June 2021

[35] "Facebook buys CrowdTangle, the tool publishers use to win the internet," The Verge, 11 November 2016, https://www.theverge.com/2016/11/11/13594338/facebook-acquires-crowdtangle

[36] "About social issues," Facebook, retrieved 24 September 2021, https://www.facebook.com/business/help/214754279118974?id=288762101909005

Our experience with social media companies and their executives is best described by their playbook: to deny blame, deflect criticism, delay change, all while raking in dollars. Big Tech continually shifts the responsibility of content moderation on their platforms to users and independent researchers with limited access, then aggressively counters any critiques or findings that researchers unearth.

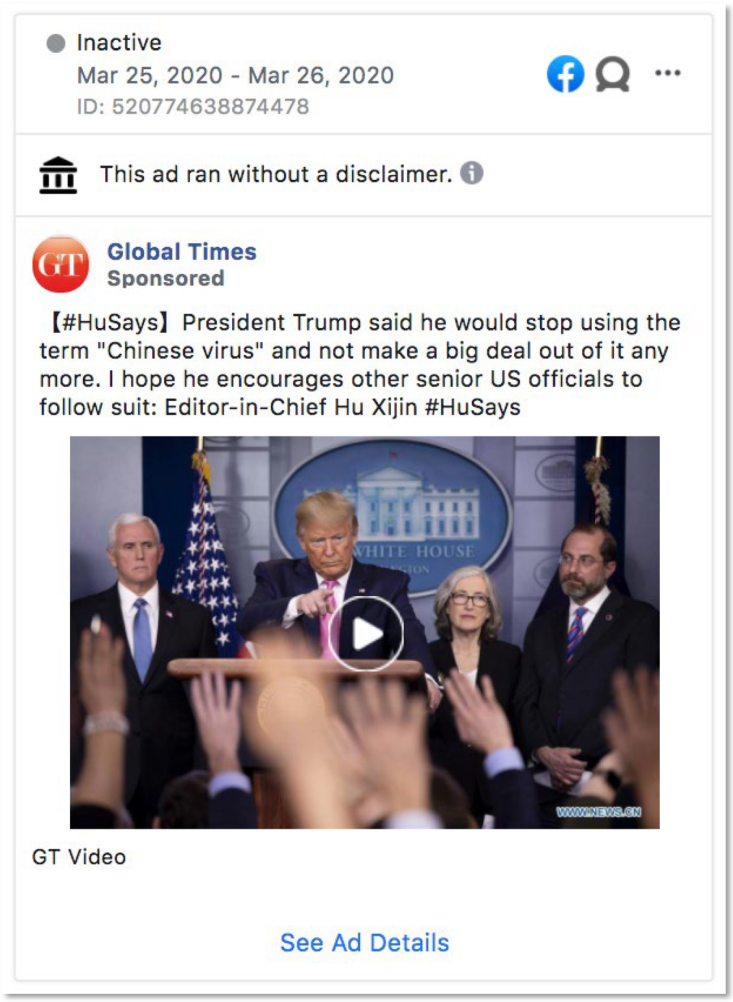
Content circulating on the largest platforms plays an outsized role in shaping the terms of public discourse, and so these platforms have a special responsibility to be transparent about the content that is most viewed and most engaged with, especially if it is harmful content such as dangerous vaccine misinformation or racist hatred.

In light of maneuvers to hamper and, in some cases, completely silence research in the public interest, we believe it is unsustainable to continue down a path of self-regulation and transparency-by-choice. Researchers need protections from companies that can revoke access and cherry-pick available data at will.

As recent reporting based on leaked information has demonstrated, Facebook now ranks alongside Big Oil, Big Tobacco, and opioid pharmaceutical companies in their internal awareness of how harmful their product is, their immense efforts to extinguish any inquiries into its harms, and the scale of just how damaging these products are to public and societal health. The public deserves access to the facts - not just the facts that Facebook chooses to release.

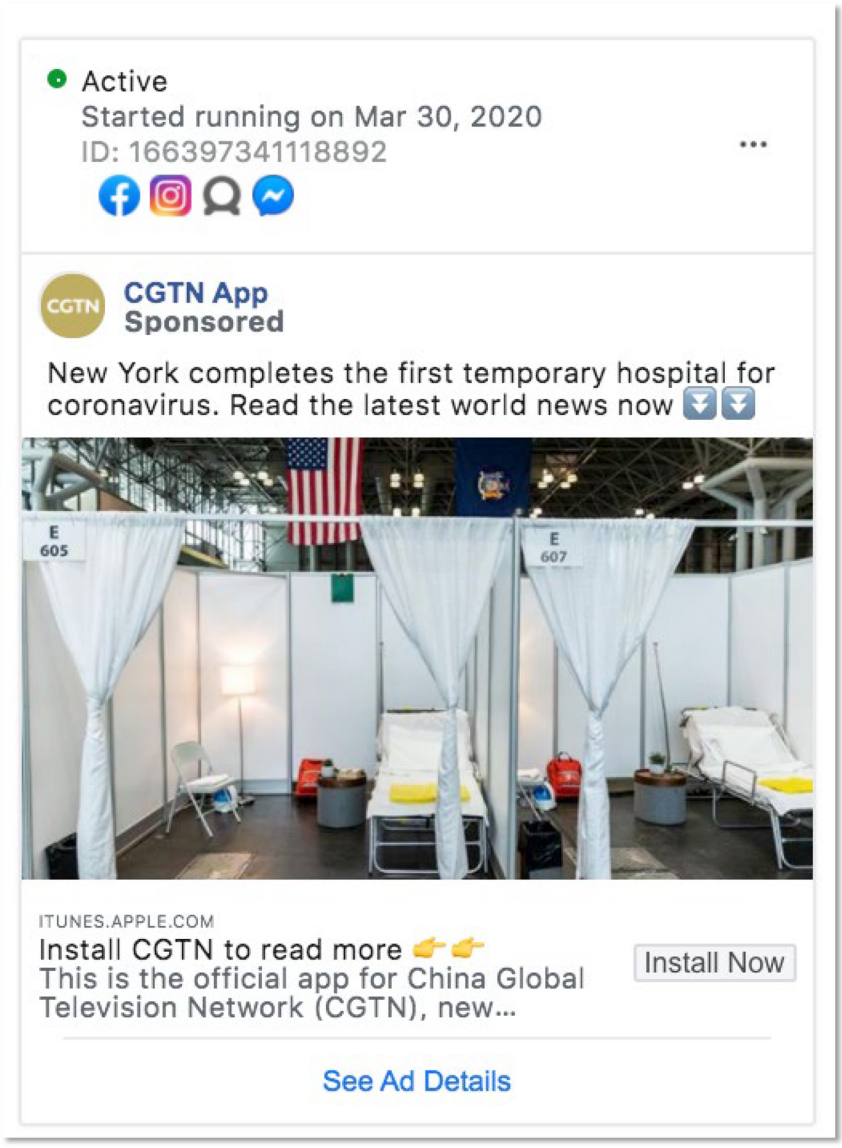
--Imran Ahmed, Chief Executive Officer, Center for Countering Digital Hate

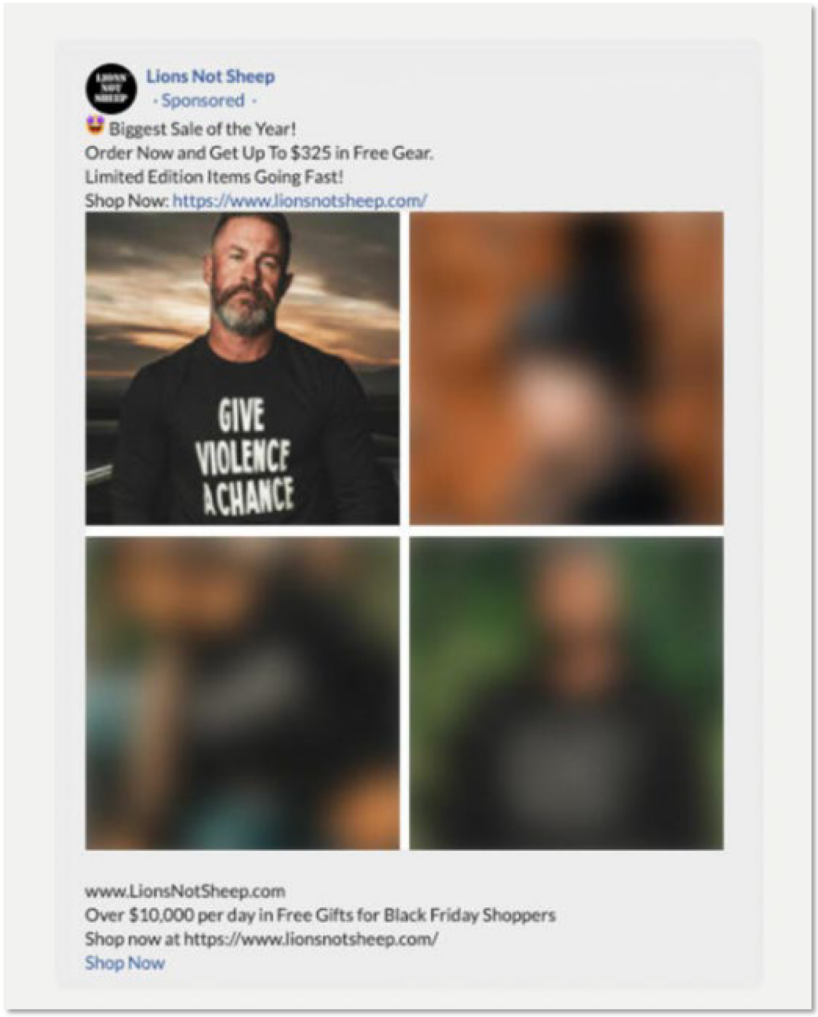
VISUALS SUBMITTED BY MS. LAURA EDELSON



Chinese-backed state media outlets routinely escape disclosure

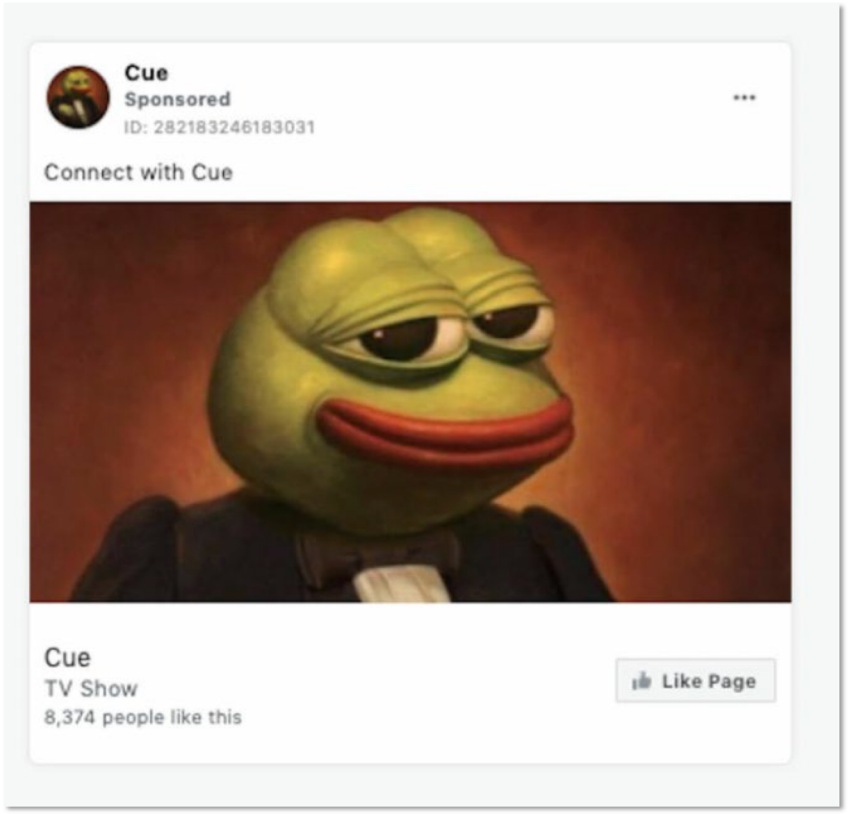

Active
Started running on Apr 27, 2020
ID: 237797864201420
CGTN App
Sponsored
Georgia among first states to reopen for business.
Read the latest world news now ⏬⏬
EASING RESTRICTIONS
ITUNES.APPLE.COM
Install CGTN to read more 👉👉
This is the official app for China Global Television Network (CGTN), new...
Install Now


Active
Started running on Mar 30, 2020
ID: 166397341118892
CGTN App
Sponsored
New York completes the first temporary hospital for coronavirus. Read the latest world news now ⏬⏬
E 605
E 607
ITUNES.APPLE.COM
Install CGTN to read more 👉👉
This is the official app for China Global Television Network (CGTN), new...
Install Now
See Ad Details

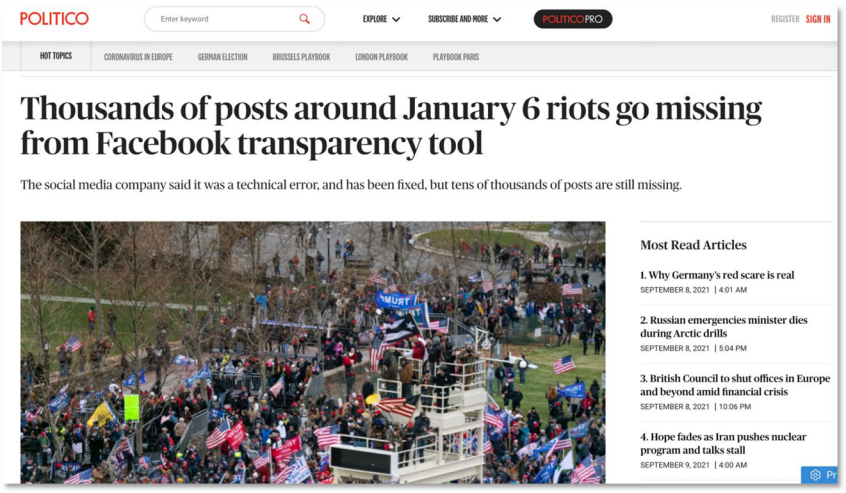


This ad ran after Facebook banned militia-related content.

Facebook took down this job ad after the Markup reported it was targeted toward African-Americans



This ad ran days after
Facebook banned QAnon content.



We discovered this bug using CrowdTangle–Facebook has cut off our access to this tool.

LETTER SUBMITTED BY ACCOUNTABLE TECH, ET AL.

Sept. 27, 2021

TO: The Honorable Eddie Bernice Johnson
The Honorable Frank Lucas
The Honorable Bill Foster
The Honorable Jay Obernolte

RE: Facebook's Stonewalling of Research into its Role in the Capitol Insurrection

--

Chairwoman Johnson, Ranking Member Lucas, Subcommittee Chairman Foster, Subcommittee Ranking Member Obernolte

We are writing to express our consternation over Facebook's flagrant disregard for transparency and our democracy, most recently by deplatforming NYU researchers hours after learning they were studying the company's role in spreading disinformation related to the January 6th Capitol insurrection[1].

While there is overwhelming evidence that Facebook was negligent as its platform was weaponized to help incite and plan the insurrection – including evidence compiled by an internal Facebook task force[2] and in federal court documents[3] – the company has failed to evaluate how their platform may have helped facilitate the Capitol insurrection, despite calls to do so from the public[4], Congress[5], and even their own carefully curated Oversight Board[6].

When Facebook initially deplatformed the NYU researchers, they claimed it was in service of protecting people's privacy. They falsely insinuated their action was mandated by the terms of the 2019 consent decree imposed on them by the Federal Trade Commission (FTC), before being forced to acknowledge that was not the case[7]. They dishonestly claimed[8] the NYU team's browser extension was a privacy threat – and yet despite establishing that false pretense, their action was *not* to block the tool, but to sanction the independent researchers[9].

---

[1] Vice News, "Facebook Just Suspended the Accounts of Some of Its Biggest Critics," David Gilbert, August 4, 2021, https://www.vice.com/en/article/n7bkg8/facebook-just-suspended-the-accounts-of-some-of-its-biggest-critics
[2] BuzzFeed News, "Facebook Knows It Was Used To Help Incite The Capitol Insurrection," Craig Silverman, Ryan Mac, and Jane Lytvynenko, April 22, 2021, https://www.buzzfeednews.com/article/craigsilverman/facebook-failed-stop-the-steal-insurrection
[3] Business Insider, "In court documents about the pro-Trump riots at the Capitol, Facebook is cited far more than any other social network," Ben Gilbert, February 8, 2021, https://www.businessinsider.com/facebook-capitol-riots-arrests-parler-instagram-youtube-2021-2
[4] The Hill, "Tech groups urge Congress to 'dig deeper' on Facebook role in Capitol riot," Rebecca Klar, July 26, 2021, https://thehill.com/policy/technology/564830-tech-accountability-groups-urge-congress-to-dig-deeper-on-facebooks-role-in
[5] Just Security, "Senate Report on January 6 Points to Need to Investigate Role of Social Media in Insurrection,"Justin Hendrix, June 9, 2021, https://www.justsecurity.org/76829/senate-report-on-january-6-points-to-need-to-investigate-role-of-social-media-in-insurrection/
[6] CNN, "Facebook told to investigate its role in insurrection," Donie O'Sullivan, May 6, 2021, https://www.cnn.com/2021/05/06/tech/facebook-oversight-board-insurrection/index.html
[7] Wired, "Facebook's Reason for Banning Researchers Doesn't Hold Up," Gilad Edelman, August 4, 2021, https://www.wired.com/story/facebooks-reason-banning-researchers-doesnt-hold-up/
[8] Mozilla, "Why Facebook's claims about the Ad Observer are wrong," Marshal Erwin, August 4, 2021, https://blog.mozilla.org/en/mozilla/news/why-facebooks-claims-about-the-ad-observer-are-wrong/
[9] Wired, "Facebook's Reason for Banning Researchers Doesn't Hold Up," Gilad Edelman, August 4, 2021, https://www.wired.com/story/facebooks-reason-banning-researchers-doesnt-hold-up/

It is increasingly clear that Facebook is actively working to prevent any investigation into their platform's role in the January 6th insurrection, suggesting they have something to hide.

And this incident can't be examined in a vacuum. It is imperative to consider the stark reality that the platform is still awash with dangerous election lies[10] unchecked by reality, that the company's efforts to shield critical data from researchers is ubiquitous, and that every way to get data from Facebook is controlled by Facebook.

That must change if we are to quell their continued assaults on our information ecosystem and protect our democratic process. We urge Congress to demand that Facebook immediately restore the NYU researchers' accounts and submit to a complete independent audit of its role in the Capitol insurrection to ensure similarly horrific events do not happen in 2022, 2024, and beyond. Our country depends on it.

Signed,

Accountable Tech
ADL (the Anti-Defamation League)
American Family Voices
Broward for Progress
Center for American Progress
Center for Countering Digital Hate
Common Sense Media
Damian Collins MP, Co-Founder of the International Grand Committee on Disinformation
Decode Democracy
Fair Vote
Fight for the Future
Free Press
Friends of the Earth
Indivisible Hawaii
Indivisible Ulster
Institute for Strategic Dialogue
Jessica J. González, Co-CEO, Free Press
Liberation in a Generation
Media Matters for America
Progress America
Real Facebook Oversight Board
Roger McNamee, Author of Zucked: Waking Up to the Facebook Catastrophe
Safiya Noble, Author, Algorithms of Oppression
Secure Elections Network
Stop Online Violence Against Women Inc.
SumOfUs
Tech Transparency Project
The Connector
Tierra Común
Women's March

---

[10] Tech Transparency Project, "False Election Audit Claims Surge on Facebook," August 5, 2021, https://www.techtransparencyproject.org/articles/false-election-audit-claims-surge-facebook

○