

S. HRG. 117-888

PLATFORM TRANSPARENCY: UNDERSTANDING THE IMPACT OF SOCIAL MEDIA

HEARING BEFORE THE SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW OF THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

MAY 4, 2022

Serial No. J-117-60

Printed for the use of the Committee on the Judiciary



www.judiciary.senate.gov
www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

56-698

WASHINGTON : 2026

COMMITTEE ON THE JUDICIARY

RICHARD J. DURBIN, Illinois, *Chair*

PATRICK J. LEAHY, Vermont	CHARLES E. GRASSLEY, Iowa, <i>Ranking Member</i>
DIANNE FEINSTEIN, California	LINDSEY O. GRAHAM, South Carolina
SHELDON WHITEHOUSE, Rhode Island	JOHN CORNYN, Texas
AMY KLOBUCHAR, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TED CRUZ, Texas
RICHARD BLUMENTHAL, Connecticut	BEN SASSE, Nebraska
MAZIE K. HIRONO, Hawaii	JOSH HAWLEY, Missouri
CORY A. BOOKER, New Jersey	TOM COTTON, Arkansas
ALEX PADILLA, California	JOHN KENNEDY, Louisiana
JON OSSOFF, Georgia	THOM TILLIS, North Carolina
	MARSHA BLACKBURN, Tennessee

JOSEPH ZOGBY, *Chief Counsel and Staff Director*

KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

CHRISTOPHER A. COONS, Delaware, *Chair*

SHELDON WHITEHOUSE, Rhode Island	BEN SASSE, Nebraska, <i>Ranking Member</i>
AMY KLOBUCHAR, Minnesota	LINDSEY O. GRAHAM, South Carolina
MAZIE K. HIRONO, Hawaii	JOSH HAWLEY, Missouri
JON OSSOFF, Georgia	JOHN KENNEDY, Louisiana
	MARSHA BLACKBURN, Tennessee

CASSIE FIELD, *Democratic Staff Counsel*

JULISSA MILLIGAN WALSH, *Republican Staff Counsel*

CONTENTS

OPENING STATEMENTS

	Page
Coons, Hon. Christopher A.	1
Sasse, Hon. Ben	2
Klobuchar, Hon. Amy	4

WITNESSES

Haidt, Jonathan	12
Prepared statement	35
Harper, Jim	14
Prepared statement	47
Keller, Daphne	10
Prepared statement	70
Persily, Nathaniel	8
Prepared statement	92
Silverman, Brandon	6
Prepared statement	107

**PLATFORM TRANSPARENCY:
UNDERSTANDING
THE IMPACT OF SOCIAL MEDIA**

WEDNESDAY, MAY 4, 2022

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

The Subcommittee met, pursuant to notice at 2:03 p.m., in Room 226, Dirksen Senate Office Building, Hon. Christopher A. Coons, Chair of the Subcommittee, presiding.

Present: Senators Coons [presiding], Klobuchar, Ossoff, Sasse, Hawley, and Blackburn.

Also present: Senators Padilla and Cruz.

**OPENING STATEMENT OF HON. CHRISTOPHER A. COONS,
A U.S. SENATOR FROM THE STATE OF DELAWARE**

Chair COONS. This hearing will come to order. I'd like to thank all of our witnesses for participating today. I'd also like to thank Ranking Member Sasse and his staff for working with mine to put this hearing together on a consensus basis. This is a critical topic, and I'm looking forward to a productive conversation today.

Social media companies, as we all know, play an enormously important role in our lives and in our society. They have helped to connect billions of people across the world and deliver a whole range of new and innovative services in ways that provide tremendous value to individuals, families, and communities. At the same time, there are critical questions about the potentially negative effects these platforms may have—concerns about propagation of misinformation, incitement to violence, or serious impacts on self-concept or mental health.

A central issue that we face in confronting these questions, whether as a consumer, as a parent, or policymakers is what are the facts? What are the actual facts? Right now, we don't really have a well-grounded data-driven understanding of how social media platforms are impacting us in our society. The reality is the vast expanses of human interaction that occur on any given large social media platform can be studied and analyzed really only by that platform. It's a problem, and it's why, in my view, we need to promote greater transparency.

Transparency is important for consumers and the public who should know how a platform they're choosing to engage with is po-

tentially affecting them. Transparency is important for policy-makers so we can better write whatever rules may regulate these platforms going forward. And transparency, I would argue, is important for the platforms themselves, because transparency itself is a positive means to promote change.

Greater transparency can address the deeply-rooted market failure of imperfect information. We've seen how public disclosure of internal research or other data can create a conversation, can alter consumer behavior, or lead to regulatory scrutiny, and then initiate market pressure that leads platforms to adjust their behavior in potentially positive ways.

On top of all of that, I think pursuing greater transparency is, and should be, nonpartisan. All sides, all points along the political spectrum, have questions that can be answered by greater transparency. Some of the most pressing topics, like the effects platforms have on our children's mental health, transcend political affiliation. This hearing will explore how to bring about greater transparency. What are the right pathways? What are the questions that we have and we need to ask and answer?

Last winter—late last winter, I released a discussion draft of the Platform Accountability and Transparency Act, known by the catchy acronym PATA with Senators Portman and Klobuchar. That draft bill would provide for transparency by creating, at first, a provision to require platforms to make certain key information available to the public on an ongoing basis—high-level information about ads, and algorithms, and widely viewed content. Second, a mechanism for data access by truly independent researchers, through the National Science Foundation and Federal Trade Commission. And third, a safe harbor so that researchers conducting research in the public interest need not fear legal action from platforms.

We released this bill as a discussion draft, knowing that it raises important questions. I look forward, in this hearing, to discussing those questions as well as many others, alongside my Ranking Member. I think those questions include making sure we're striking the right balance between privacy and transparency, and appropriately also weighing what colleagues are doing on these issues in Europe, and what legislation may arise in the States.

Of course, PATA is not the only bill out there to address these issues. I want to thank some of my colleagues, Senators Blumenthal and Blackburn, for example, for their work on the Kids Online Safety Act, also relevant to this discussion.

With Senator Sasse's cooperation, we have assembled an all-star panel, with a diversity of views and perspectives, to grapple with these questions today, and I look forward to it. I'll introduce you shortly, but now I'd like to turn to my colleague and friend, Senator Sasse.

**OPENING STATEMENT OF HON. BEN SASSE,
A U.S. SENATOR FROM THE STATE OF NEBRASKA**

Senator SASSE. Thank you, Chairman, and thank you to all five of our witnesses for participating today. I want to applaud Chris for his leadership, and his team, for focusing on an incredibly important issue. We're here to talk about transparency on social

media, which is another way to say how do we understand the role social media platforms play in our lives, in our families, and in society more broadly?

There's no question that social media has changed American society. My colleagues on both sides of the aisle have serious concerns about how social media has changed the country, although their concerns are often quite diverse in what they think they're aiming at. My Democratic colleagues are often concerned with whether social media platforms take down enough posts that they think are harmful. And many of my colleagues on this side of the aisle spend a lot of time arguing that social media companies should stop censoring speech with which they differ. And most of the time, the people making these arguments are talking far past each other, and the sense that there's consensus about what to do is really just consensus that something is wrong, because we can't even agree on some of the basic facts about what content moderation is, how it works, how it should work. It is not surprising that we can't see eye to eye on these facts, because frankly, we don't understand the platforms very well. Congress is often undereducated about how these things work, and you're going to help us learn more today, and we're grateful for that.

Social media companies have opaque policies that are applied inconsistently, and there often seems to be one set of standards for the wealthy and the well-connected, and another set of standards for everyday Americans. As I've said before, I'm pretty skeptical that turning to the Government is necessarily going to fix many of these problems, but there are things we should certainly start to do to understand the problems better together.

What we do know is that a lot about social media is complicated and has negative effects. One of the most important things we know is that social media companies have a business model that exists to maximize engagement. It's a pretty basic truth, but when we get to a lot of the screaming about what legislation might or might not fix the problem, we first need to admit that the business model of these companies is to maximize engagement, and social media algorithms, and company policies, and business decisions are ultimately designed to keep people on platforms for as long as possible.

So, it should come as no surprise to many of us that social media is habit-forming over time. For some, it slips into something that should rightly be called addiction. And as we've integrated social media more deeply into our lives and our institutions, most of us haven't stopped long enough to ask, what habits are we forming? What loves are we developing? And are these good and healthy habits? How do our social media habits impact our families and our kids, on the one hand, and our politics and our political, and social, and cultural institutions on the other?

So, let's start with families and kids. Ask just about any parent of a teenager whether they worry about social media, and whether it's impacting their kids, and almost all parents, but especially parents of teenaged girls, almost immediately begin telling a story that's worrying to them, and they start talking about things they've seen social media do to impact and influence their kids.

Like a lot of parents, Melissa and I worry about our three. We want to raise our daughters to be strong, confident women who will love their neighbors and serve the world. We want them to know their worth and understand their identity, their purpose, and their value, which is infinitely more than you'll ever get on social media's infinite scroll.

I've often joked that I'd prefer my 11-year-old son steal the keys to the pickup and go joyriding with an open bottle of bourbon than to wander with a smart phone, unmanaged, unattended, on the internet. It's a joke, but it's not a joke, because these are serious, lifelong, identity-warping forces at play. We have also seen a lot of new neurobiological research, which I won't try to summarize in this slot because we have Jonathan Haidt here, who is much better qualified than almost anybody on earth to talk about this.

Social media also poisons our political discourse. One of the most important ways that social media platforms maximize engagement is by sending users two powerful, unending messages: You're right, and everyone who disagrees with you is evil. Platforms show Americans the news, posts, and commentary that they already agree with on the one hand, and they amplify the most outrageous behavior by crazy partisans on the other side. This creates echo chambers where political weirdos are mostly just talking to political weirdos with their certainty that all political weirdos are only on the other side. It turns out, the weirdness is mostly driven by being addicted. It isn't mostly a right/left problem. This is mostly an addiction problem, versus the vast majority of people who don't want to be addicted.

Over time in these echo chambers, people tend to adopt more and more extreme views, and then those extreme views are picked up by the other side, which claims victory for having been right all along, and having recognized that only the crazy people—only people on the other side are crazy, and the virility spiral, the polarization, continues.

As we step back and think about the role of transparency about social media platforms, we should not lose sight of the fact that we already do know quite a lot of basic introductory things about social media, and how it impacts us, and how it harms kids, families, and institutions, and how it polarizes our politics.

Hopefully today, we can learn more, and we're grateful to the five of you for helping us in that quest. Mr. Chairman.

Chair COONS. Thank you, Senator Sasse. Thank you for that insightful opening comment and several powerful visual images. I'd like to take the Chair's prerogative and invite Senator Klobuchar to give some opening remarks. She's been a great partner on developing the Platform Accountability and Transparency Act, and she has a scheduling conflict that'll prevent her from staying for testimony and questioning, but wanted to make some opening remarks. Senator.

**OPENING STATEMENT OF HON. AMY KLOBUCHAR,
A U.S. SENATOR FROM THE STATE OF MINNESOTA**

Senator KLOBUCHAR. I promise I'll look at the transcripts. Thank you so much to both of you, and thank you, Senator Coons, for your

leadership on this bill with Senator Portman. Thank you, Senator Sasse, for that great description.

I had one mom tell me that it's like she keeps trying to get control of what her kids are seeing, but it's like water that's coming out of a faucet that won't stop, and it's overflowing, and she's just standing out there with a mop, trying to do it, and she can't. And so, I think so much of this has to do with the magnification, the amplification, of what you have called this kind of polarized speech. I don't want to get your words wrong, what you just said, that. Yes. Political weirdos. Okay. There you go.

And I think what you see with that is that the influence of these platforms is just simply unprecedented. Even though these platforms are seemingly free, they're really not because you're seeing advertising, and they're making money off of you, and then they use the information they have, and then make more money off of you. In fact, a number of even looking at the data shows that they make more money off of us than other industrialized nations, just simply because we don't have any rules of the road in place.

For so long, we've been hearing, "Trust us. We've got this," and I think that that era of blind trust is coming to an end. And that's why you see the work that's going on the competition side.

I'm also on the Commerce Committee. That's why you see the work that's going on with updating some of the kids' laws, and that's why you're seeing the work that's going on on privacy, and then, of course, on algorithms, and getting more transparency.

You know, we all know that you can't yell fire in a crowded theater. That is not considered free speech. That's not considered okay. And the way I think about it is if you're a theater, okay. Someone yells fire, it's not your fault, but you better have exits so people can get out of there. But if you had speakers, and you amplified that guy yelling fire in all of your multiplex of theaters deliberately, that would be a problem if you thought somehow you'd make more money. That is kind of what we're talking about here with algorithms.

This hearing is also about how quickly misinformation and disinformation can spread online. A recent report from the Center for Countering Digital Hate identified a dozen specific content producers as the original sources of an estimated 35—65 percent of coronavirus disinformation online, where, literally, people die when this stuff is not corrected.

We need transparency because these tools can hurt millions of people. That's why this bill is so important, the Platform Accountability and Transparency Act. It will make it so companies like Facebook can't block researchers from looking into their platforms and algorithms. I note that President Obama touted the importance of this legislation in his recent speech at Stanford, and I am committed, and I know Senator Coons is, to seeing this through.

So, I want to thank all of you. I look forward to reading your testimony, and I know that my staff will be here as well. So thanks for coming before us today.

Chair COONS. Thank you, Senator. Today, we welcome five witnesses to testify about the need, the value, the importance of greater transparency in social media companies, and how that can most reasonably be achieved.

Our first witness is Brandon Silverman. Mr. Silverman founded CrowdTangle, a social analytics tool used to monitor and understand how content is performing on social media platforms in real time. CrowdTangle was purchased, acquired, by Facebook in 2016, where it became an indispensable tool for journalists, fact-checkers, and external organizations. Mr. Silverman worked to implement and improve the product while at Facebook until recently departing the company.

Next, we have Professor Nate Persily. Professor Persily teaches at Stanford Law School and is the codirector of the Stanford Cyber Policy Center, Stanford Program on Democracy and the Internet, and the Stanford-MIT Healthy Elections Project.

We'll next hear from Professor Daphne Keller. Professor Keller directs the Program on Platform at Stanford's Cyber Policy Center, where her work focuses on platform regulation and internet users' rights.

After that, we have Professor Jonathan Haidt, who is testifying remotely today. Professor Haidt is the Thomas Cooley Professor of Ethical Leadership at NYU's Stern School of Business, where his work focuses on morality, emotion, and politics.

Finally, we have Jim Harper, a nonresident senior fellow at AEI, the American Enterprise Institute, where he focuses on privacy issues and select constitutional law issues.

Let me briefly lay out the mechanics after we swear in all of the witnesses. Each witness will have roughly 5 minutes to provide an opening statement. We'll proceed to questioning. Each Senator will have initially 5 minutes. Hopefully, we will have time for a second round after that. So, if you would all please stand to be sworn in?

[Witnesses are sworn in.]

Chair COONS. Thank you all. Mr. Silverman, you may now proceed with your opening statement.

**STATEMENT OF BRANDON SILVERMAN, FOUNDER AND
FORMER CEO, CROWDTANGLE, OAKLAND, CALIFORNIA**

Mr. SILVERMAN. Thank you for having me. My name is Brandon Silverman, and I was the CEO and cofounder of CrowdTangle, a social media analytics tool. We made it easy to see what was happening on social media, and we were very good at what we did. In 2016, we were acquired by Facebook, and over the next few years, we partnered with thousands of outside organizations around the world, to help them study and monitor social media, including journalists, academics, human rights activists, nonprofits, and more. By the end of 2020, the New York Times called us perhaps the most effective transparency tool in the history of social media.

However, in the spring of 2020, after an intense internal debate about whether the transparency we provided was worth it, Facebook paused all work on CrowdTangle and disbanded the team running it. I left the company shortly after.

Today, the future of CrowdTangle is up in the air, and along with it, one of the most robust and successful transparency programs that Facebook operates.

I'm here today to share what I've learned working on transparency for over 10 years, including what it's like to try and advance transparency from inside one of these large platforms, and

why I believe it's time to stop sitting back and hoping that platforms voluntarily share data, and to pass legislation that makes it safe and responsible to share data with the outside world.

In 2016, CrowdTangle was acquired by Facebook, and over the next few years, we expanded our work to a wide variety of new industries. We added new features and new data, and it became one of the most widely used tools in the industry. Our data was frequently cited here in congressional testimony over the years.

There was no shortage of use cases for what we built, but there was a limit to how far we could push transparency from inside the company. The truth is, is that it's not easy to work on transparency from inside a major platform. For one thing, it can be incredibly uncomfortable when your work, and the work of your team, are constantly fueling criticism, some fair and some not, of the company where you work. Those normally take a toll on your team, but they also make it harder to get resources, they make it more difficult to launch new features and add more data, and ultimately, they provide constant ammunition to executives who are skeptical about doing transparency at all.

On top of that, there are also organizational challenges that make it hard. There are conflicting regulatory and legal requirements all around the world that are all interpreted differently by whichever set of whatever team or lawyers you might talk to. There's the fact that no matter how much transparency you do, you're rarely going to get credit for it in the public eye. There is a constant and fierce competition for resources and the attention of leadership. And that's just to name a few. But more than all of those factors combined, the single biggest challenge is the platform—single biggest challenge is that platforms can get away without doing any transparency at all.

YouTube, TikTok, Telegram, Snapchat, these platforms represent some of the largest and most influential platforms in the United States, and they provide almost no functional transparency into their systems at all. Moreover, despite a lot of Facebook's laudatory transparency efforts, there are also incredibly significant parts of their platform that still remain entirely inside black boxes.

Today, CrowdTangle is still available, but it's in maintenance mode. Facebook has stopped onboarding new partners, no new features or major updates have been released in 2 years, and the global partnerships team that used to run it no longer exists. But while we were there, our team saw the power of transparency. Almost every single day, our team saw examples of partners using social media data to help protect elections, prevent real-world violence, fight global pandemics, empower independent journalism, hold platforms accountable, and more. We saw how transparency can be a tool to make sure that social media lives up to the promise of strengthening free and open societies, instead of being used to undermine and weaken them.

I think what happened to CrowdTangle should be seen as a bellwether, and that it's too hard to make progress on these issues, at the scale and breadth we need, from inside a company. As a result, we've seen that the industry as a whole has simply not made enough progress equal to the responsibilities they have. And I don't

think there's any reason we should expect that to change going forward. If anything, I think we should expect less voluntary efforts.

That's why I believe it's time to create legislation that makes data sharing and transparency a requirement for entire industry, and creates mechanisms to do it in safe and responsible ways. I think the Platform Accountability and Transparency Act represents an important step in the right direction. There are real challenges to getting this legislation right, and we're going to hear about some of those today. However, if we don't find ways to move forward, we will continue to be in the dark about the real impact of social media on our lives. We'll continue jumping from one anecdotal data point to another, from one leaked document to another, from one urban myth to another without ever establishing baseline evidence-backed conclusions about the role it plays in our lives.

When I think about social media and a lot of the public discourse about the role it plays, I'm reminded of anecdote about the policeman who sees a drunk man searching for something under a streetlight and asks what the drunk man has lost. He says he lost his keys, and they both look under the streetlight together. After a few minutes, the policeman asks if he's sure he lost them there, and the man replies, "No." He lost them in the park. The policeman asks, "Well, why are we searching here?" And the man says, "This is where the light is."

For too long, our public discussion about social media has been focused on the moments where we briefly found ourselves under a streetlight. It's time to turn the lights on for good. Thank you.

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

Chair COONS. Thank you, Mr. Silverman. Professor Persily.

**STATEMENT OF NATHANIEL PERSILY,
JAMES B. McCLATCHY PROFESSOR OF
LAW, STANFORD LAW SCHOOL,
STANFORD, CALIFORNIA**

Professor PERSILY. Thank you, Chairman Coons. Thank you, Ranking Member Sasse, Senator Blackburn, and my Senator, Senator Padilla, for being here. I really appreciate testifying for this Committee again. I'm going to talk a little bit about the purposes of transparency, and then also, like Brandon, I'll talk a little bit about my experience in working with Facebook and other platforms in trying to get data out of them.

Let me begin by just saying sort of what the bottom line is here, which is that we cannot live in a world where Facebook and Google know everything about us and we know next to nothing about them. All right? And these large platforms have basically lost their right to secrecy. Their power over the information ecosystem is really unrivaled in world history. Given that, it's time for a democracy to step forward and regulate them in the public interest. The least that we can do is to get some transparency out of them so that we understand exactly what's going on.

As Senator Sasse said, the questions with respect to internet regulation are extremely complicated, very difficult, and in many respects, we don't know what the right answer is in many of these domains. But transparency is the first step to finding answers in

any of them. And we think about the purposes of transparency, it's sort of a, if you'll excuse the pun, you know, it is a meta-bill. Right? It is about enabling our ability to regulate and to act in so many other domains.

First, let me say that these firms are information monopolies. Usually, when we talk about it, we talk about it in the antitrust sense, but you know, in terms of competition and the monopoly power that they have over their economic domains. But they're information monopolies in a different sense, which is that they control all of the information which is now most revealing about social problems. Right? We've never been in that position before.

Those of us who are social scientists, when we would be analyzing data in the pre-internet age, right, most of that data was freely available, either through Government statistics, survey data, or other kinds of data. Now most of the data which is relevant to contemporary social problems is locked up in these private companies. Right? And it's only through legislation that we're going to be able to unlock it and to find out exactly how big these problems are.

But I want to emphasize one thing, and I think Senator Coons, you mentioned this before, which is yes, this is a very difficult trade-off to get right. We need to balance transparency with privacy. I think everybody on this panel, and in the Senate, is aware of that. But the question is not whether this data will be collected and analyzed, the question is whether the only people who will be able to analyze the data are the people inside the firms who are tied to the profit-maximizing mission of the firms. All right? And so, the only question that PATA and other bills like this are posing is someone who is not tied to the profit-maximizing mission of the firm going to have access and to do research in the public interest.

So, let me talk a little bit about the purposes of transparency. The first set of purposes and goals, I think, of transparency, which is sometimes undersold, is that it will actually change the behavior of the firm. To some extent, I get criticism a little bit, when you emphasize transparency, that it's seen as sort of weak legislation because it's not, you know, breaking up the companies, or it's not going right after content moderation. But once the platforms know that they are being watched, it will change their behavior. All right? They will not be able to do certain things in secret that they've been able to do up to now.

Second, as Senator Coons mentioned, I think it will lead them to change their products, right, because once we have a greater appreciation for what's actually going on in these firms, those on the outside can do research that a lot of the insiders are not doing on their products.

Second, as you both mentioned before, this will educate policymakers. It'll educate policymakers here in Congress, whether the issue is child endangerment, or disinformation, or antitrust, or privacy. It will educate our European allies who are doing much more aggressive regulation right now. Now, as well as in the States. Look at the bills coming out of Texas and Florida. As you said, we are legislating in the dark.

Then finally, it will educate the public not just about what's happening inside these firms, but also the dynamics of the information ecosystem.

As Senator Sasse was saying, there is a fundamental debate here as to what is going on. Is the problem, you know, runaway hate and disinformation, and the like, on the platforms? Is the problem platforms are overcensoring particularly conservative voices? This is what transparency is going to answer. Right? Those are the questions that we would be investigating.

I'll say just in conclusion that I spent probably 4 years of my life trying to get data out of Facebook through a program called Social Science One. The people we worked with inside the firm were fantastic. They were with us all the way. The problem was that ultimately, when it came down to providing the most robust data that those inside the firm had access to, they simply couldn't do it either because they are worried about another Cambridge Analytica, or they simply didn't understand whether the legal environment would be conducive to that.

And so, what I would say, sort of, in conclusion, is that we shouldn't have to wait for whistleblowers to whistle. Right? This is something—this type of transparency legislation is about empowering outsiders to get a better idea of what's happening inside these firms.

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

Chair COONS. Thank you, Professor. Professor Keller.

**STATEMENT OF DAPHNE KELLER, DIRECTOR, PROGRAM ON
PLATFORM REGULATION, CYBER POLICY CENTER, FREEMAN
SPOGLI INSTITUTE FOR INTERNATIONAL STUDIES,
STANFORD UNIVERSITY, STANFORD, CALIFORNIA**

Professor KELLER. Thank you for the opportunity to testify. I work on platform regulation, which as Senator Sasse referenced, is really complicated. It's exciting to be able to testify about a topic where I think there's actually a viable way forward. I'm particularly honored to speak beside Brandon Silverman and Nate Persily, both of whom have built actual, real-world, functioning transparency models. I'm also excited to talk about this at a time when the EU has just moved forward on platform transparency in a dramatic way under the Digital Services Act, or DSA. I think that is really paving the way for a whole new era of platform transparency.

I think today, we will hear about a real diversity of transparency tools, and that range of tools is what we need. Not every approach is useful for every research topic, or even for the way that every platform functions. As someone who has worked with multiple approaches to platform transparency, going back over a decade, including in-house at Google, I would like to find a way to enable a whole range of these approaches.

This includes fixing the laws that constrain so-called scraping of data from public websites. This is kind of low-hanging fruit and would have the side effect of helping with some interoperability and competition goals. It also includes building APIs, which are just channels for computers to talk to each other, so people re-

searching things like bias and algorithms can submit bulk queries and look at bulk results. It includes the kinds of mandatory disclosures contemplated in laws like the discussion draft of PATA. All of this can vastly improve public information, both about online harms and about what regulatory responses will actually make things better.

To make these laws work, though, there are some pitfalls we need to navigate. Some are practical, some are constitutional, some are political. My written testimony on this was very long. I'm sorry. It raised a lot of questions that I think appropriately should go to an agency, because they are in the weeds, and they're iterative, and they will change with technology. But it also raised questions that I think are serious policy decisions that are Congress' job to resolve. So, I'm going to talk about those a little more here.

One is about privacy and surveillance. For researchers to examine what is being said, and claimed, and propagated online, and how platforms influence that, they will need to look at information about people. There are unavoidable tradeoffs in deciding how much they get to do that. Sometimes, I think the need for public information should be paramount. Other times, user privacy should. This is something where Congress should provide guidance ideally through Federal privacy legislation. If you have to resolve it here, you know, it deserves attention.

When it comes to Government surveillance, though, so not the researchers, but, you know, law enforcement getting access to data, I think there is a brighter line. Nothing about these transparency laws should change Americans' protections under the Fourth Amendment, or laws like the Stored Communications Act. I don't think that's anyone's intention here, but clear drafting is essential to ensure that Government can't effectively bypass Fourth Amendment limits by harnessing in the unprecedented surveillance power of private platforms.

A second issue is about competition and the practical cost and benefits of using different transparency tools for different companies. Laws designed for a Google or a Facebook are a bad fit for companies that are far smaller in measures of revenue, or users, or employees. Those companies may not actually be relevant for the problems that laws like this are trying to solve. I don't think we need a live dashboard showing us which hotels are most popular on Tripadvisor, for example. Hopefully, the problems of designing rules for giant incumbents, and then applying them to a whole competitive ecosystem, speak for themselves.

The third issue is about CDA § 230. I hate to bring it up, but as I mentioned in my testimony, I don't think tying transparency obligations to CDA § 230 solves the problems even that CDA § 230's critics want to solve. I think, instead, it sort of opens the door to very unpredictable litigation.

The last thing is the First Amendment. I want transparency mandates to be constitutional, but there are serious challenges, and I hope that you will put really good lawyers on that because I want this thing to work.

So, those are my concerns. In platform speak, these are the things to solve before launch, and I'm happy to answer any questions about the many other things I wrote about later on.

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

Chair COONS. Thank you very much, Professor Keller. I believe we're now going to have remote testimony from Professor Haidt.

**STATEMENT OF JONATHAN HAIDT, THOMAS COOLEY
PROFESSOR OF ETHICAL LEADERSHIP, NEW YORK
UNIVERSITY STERN SCHOOL OF BUSINESS,
NEW YORK, NEW YORK.**

Professor HAIDT. Hello. Greetings. I hope you can hear me properly. It's an honor to be testifying here. Senator Coons, you're absolutely right that this issue of transparency is completely non-partisan. Senator Sasse, you're absolutely right that all of us with teen kids, myself included, are concerned about this. We don't know what's going on, but the kids are getting sick and we want to know, is this the cause? And Senator Klobuchar, yes. The era of blind trust is coming to an end.

I'm a social psychologist. I study morality. I've studied moral development. I began to notice that something was going really wrong with teenagers, entering college students, around 2014. By 2015, it was clear all of our mental health centers were flooded on campus. A few years later, it became clear there is an epidemic of depression and anxiety sweeping across the United States for teenagers.

What I'd like to do in my remarks here is to make—I want to give you a distillation of the facts that I have aggregated on what's the nature of the teen mental health crisis. Then second, what is the evidence, the empirical evidence, that this is caused, in part, by teens suddenly moving onto social media en masse around 2011.

All of my testimony, I submitted in the PDF file that is submitted with my testimony, I have links to two collaborative Google documents where I've invited other experts to critique, to say what are we missing. We have relatively complete listings of the studies on all sides here.

Let me begin. Part one. The specific, gigantic, sudden and international mental health crisis. I'll just make these six points. You can find elaboration of them with graphs and links in the submitted testimony.

First, the crisis is specific to mood disorders. This is not an across-the-board increase in all kinds of mental health problems. It's specific to anxiety and depression, and the behaviors that go along with them, which is especially suicide and self-harm.

Second, the crisis is not the result of changes in the willingness of people that self-diagnose. As late as 2018, some experts were still saying, "It's not real. It's just, you know Gen Z, they're more comfortable talking about depression. It's not a real thing." Now it's clear it is, again, because of the very sudden increase in depression, I'm sorry—in hospital admissions for self-harm and completed suicides. All of that goes way up in the early 2010s. The self-harm lines are quite dramatic. Relatively flat, and then right around 2010, boom, they start skyrocketing upwards.

Point number three, it came on very suddenly. This was not a gradual curve up.

Point number four, the increases are very large. We're not talking 10 or 20 percent. Depending on what you look at, it's anything

from 50 to 150 percent. Self-harm for young teen girls in particular is up more than 150 percent, in fact, 180 in the last data that I saw. These are enormous, sudden increases.

Point number five, the crisis is gendered. Boys and girls both have plummeted mental health since the early 2010s, but the girls have fallen further on some measures. On others, they're about the same percentage wise but the girls starting rates of anxiety and depression are higher, so the increase is a much larger number of girls. So, the crisis is gendered.

The sixth point, the crisis has hit many countries. It's not just the U.S.A. The patterns in Canada and the UK are identical to those in the U.S., and Jean Twenge, and I, a professor at San Diego, have published a study showing that actually, across the world, loneliness at school also went up after 2012.

Those are the points that I want to make about the mental health crisis. It is real. It is big. It is sudden. It is gendered.

Now what's the evidence that social media is a cause? The first point is that correlational studies consistently show a link between heavy social media use and mood disorders, but the size of the relationship is disputed.

Point two, you will often hear from experts, "The size is so tiny, it's no bigger than the correlation of mental health problems with eating potatoes or wearing eyeglasses." But this is not true. In the main study that found that, which I talk about in the submitted testimony, that's the relationship for all digital media use. This is very important. When you hear people talk about studies, usually, it's about all digital media use, including watching Netflix, with mental health outcomes. Those correlations are, indeed, tiny.

But, and this is point number three, when you zoom in and look just at the relationship between social media use and mental health outcomes, the correlation is much bigger. There's an emerging consensus that it's between $r = 0.1$ and 0.2 . It's in that range.

Point number four, those correlations are even larger for girls. Probably closer to 0.2 . $r = 0.2$.

Point number five, the effect size is even bigger during puberty. A recent study showed between 11 and 13, girls are especially likely to be harmed by being on social media. We must try harder to protect puberty. Get this stuff out of middle school, for God's sakes.

Point number six, correlations of 0.1 to 0.2 are not small. This is what public health matters are mostly about, the correlation of childhood exposure to lead with adult IQ is 0.09 . There's a new realization amongst psychologists that small effects played out over millions of people over many years, add up to gigantic public health crises as we have with lead and water.

Point number seven, there's experimental research as well. This is not just correlational. The experiments mostly show that if you randomly assign people to conditions, reducing social media use tends to have beneficial effects.

Point number eight, the eyewitness testimony is there. We asked the kids, as Facebook did, and what they found, Facebook's own research found that teens blame Instagram for increases in the rate of anxiety and depression. This reaction was unprompted and consistent across all groups.

I'm going to conclude by saying, along with the others who have been testifying here, we really, really need to see the data. We must have platform accountability and transparency. Imagine that all of our kids began eating a certain kind of candy that had never existed before in 2011. All of them were eating this all day long, and in 2012, they started developing leukemia in large numbers. And some people said, "Well, you know, correlation is not causation. We can't be sure. We can't be sure." Okay, fine. We can't be sure, but can we at least compel the candymaker to tell us what our kids are eating?

Thank you.

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

Chair COONS. Thank you. I very much look forward to continuing our conversation and appreciate the structured and engaging way in which you delivered those remarks. Mr. Harper, if you might, you're our final witness today.

**STATEMENT OF JIM HARPER, NONRESIDENT
SENIOR FELLOW, AMERICAN ENTERPRISE INSTITUTE,
WASHINGTON, DC**

Mr. HARPER. Thank you, Senator Coons and Senator Sasse. Thanks for the opportunity to testify today. This hearing, and the Platform Accountability and Transparency Act, raise many interesting issues.

When I finished writing my 22-page testimony, I thought I had barely scratched the surface. I also thought mine would be the longest, but I lost.

[Laughter.]

We're all in favor of transparency. I've done a good deal of work on Government transparency over the years, as detailed in my testimony, and I always hoped for more. The bulk of my attention over the last two decades, though, has been on privacy.

I'm sorry to play skunk at the garden party a little bit, here, but there are very high privacy costs, I think, to the mandated disclosure regime found in PATA. I see no limit on the subject matter of data held by platforms that the legislation affects. It would allow the National Science Foundation and Federal Trade Commission to take essentially any data from platforms, to give to approved researchers. In my opinion, this runs contrary to an emergent property rights regime that is an important protection for consumers and their privacy.

My belief is that platforms and communications providers make contractual promises to protect privacy in their privacy policies and in their terms of service documents. In doing so, they also divide up nascent and property rights in data. In the bundle of sticks model of property taught in law school, the right to exclude others from personal information remains with the consumer, subject to narrow exceptions like protection of the platform itself, response to law enforcement, and so on.

Across the legal landscape, there are strains of recognition that this is the case, including in the Supreme Court. If congressional legislation took data from platforms to give to researchers or anyone else, it would cut against the grain of this trend. It would treat

data held by platforms, including data held as a bailment or in trust for users, adds so much soup in a tureen waiting to be ladled out. The legal immunities in the PATA legislation further erode confidence that privacy will be protected in a mandated disclosure regime.

An unconstrained disclosure mandate may also be unconstitutional. The Supreme Court appears likely to revive the nondelegation doctrine soon, and in an unrestricted grant of authority to mandate disclosure for the all-purpose, but unfortunately nebulous goal, of transparency, may not survive it.

That's not just a constitutional point, I don't think, but it's a prudent one. We don't know what the future holds for our politics, and we don't know what type of data a future administration might use the NSF and FTC to order from platforms about Americans, our habits, and our communications.

I also specifically recommend, in my written testimony, against bringing transparency to platforms' moderation practices and to their security efforts, both how they secure themselves and how they provide security to their users. The PATA legislation considers this. It provides for privacy and security regulations pertaining to the mandated disclosure of data, but the mandatory disclosure regime itself would increase vulnerabilities and the attack service, as they say, in computer science, of the systems. Moderation and security systems are constantly probed by bad actors, who want to turn platforms to their own ends or just ruin them. Mandated disclosure would create new opportunities for wrongdoing.

I'll say this, since reading my colleagues' testimony and some of the authorities they cite, I'm less enthusiastic about my written testimony on the First Amendment issues. I am taken by the breadth of the data seizures made by possible by PATA, and my frame of reference is Fourth Amendment privacy. There are areas where Government requires businesses to disclose or publish information about themselves. This is not the case, though, I think, where that includes the editorial choices of institutions engaged in free speech.

The internet and social media are strange, but real, descendants of the printing press, disembodied and given to everyone to use as much as they want. Social media companies aggregate and augment this mass exercise of expression. I think it's well within precedent to regard what they do editorially as protected by the First Amendment.

Where disclosure mandates exist, you can probably find a close fit between means and ends. When auto dismantlers are forced to reveal their inventories and sources, that makes them much less likely to become fencing operations. Requiring audited financial statements from public companies prevents various forms of fraud. So far as I'm aware, and unfortunately, platform transparency through disclosure mandates does not have that kind of tight nexus with recognizable protections or social gains.

Professor Haidt's testimony, reading it, you know, the effects of social media on teen girls, that natively powerful testimony, and that's important stuff. He is especially credible to me because of his work through various organizations to strengthen academic inquiry norms and honest debate. I would like it if transparency could di-

rectly fix the problems he cites, or make our democracy evidentially more functional, but the benefits of transparency, unfortunately, are contingent and remote, where the privacy losses are immediate and, I think, real.

The solutions to all of these problems will be years in coming, and they will come from a wide variety of adaptations and sources, university research being just one contributor.

This hearing has helped emphasize the importance of transparency. I don't think, unfortunately, that it lays much groundwork for a mandatory disclosure regime like the one found in PATA. It's excellent to have had a discussion draft, though, to work from.

Thanks very much.

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

Chair COONS. Thank you. I'd like to thank all of our witnesses today for your thoughtful testimony. This is exactly the sort of broad-reaching hearing I was hoping we would have, and I am excited that the vote has not yet been called, and so we may have a little more time to explore it. I particularly appreciate the perspectives offered on transparency, the potential ways to achieve it, questions about its cost and the cost benefit.

I'm going to start my questioning by setting the scene a little bit and exploring various pathways toward greater transparency, which, I believe, would be beneficial, bipartisan, and the role that Congress should play. We may well take a second round, depending on what happens with votes.

If I might, first, Professor Persily, I appreciate the point you made about how transparency can transcend political ideology and might be, I think as you said, a bipartisan first step on the road to sounder policy. Could you say more about the kinds—the kinds of questions independent researchers might answer with greater access, and how answers to those questions might, in a more immediate way, deliver on the promise of better policymaking?

Professor PERSILY. Thank you for that. There is a fundamental disagreement between conventional wisdom and what the platforms is happening on their services. For example, we have no sense of the prevalence and size of the problem of hate speech, disinformation, incitement, child endangerment, and the like. If you ask the folks at the platforms, they will say, for example, that a lot of the interpretations that were made off of CrowdTangle data, which looks at different engagement metrics and the like, that that was misleading. That actually, the average person's experience is not one which is replete with hate speech, disinformation, and the like. That's an empirical question. If we had access to the data, we would be able to figure out how big a deal some of these problems are in the average person's newsfeed.

And not just the average person, because I think Senator Sasse was exactly right when he was talking about weirdos in his opening comment. Part of the question is not just what the average user sees, but how concentrated minorities of users, what rabbit holes they may be going down.

That also is a second area of inquiry which is open for debate. What role are the algorithms playing in sending users down rabbit holes of polarization, conspiracy theories, and the like? On the out-

side, it's conventional wisdom right now that the algorithms are having a huge impact in doing so. If you ask the folks of the platforms, they say no. That's not actually what's happening. If anything, the algorithms are putting them toward more moderate content. We can answer that question, right, if you just give us access to some of the same data, we can figure it out.

Finally, particularly on the issue of censorship and whether the content moderation practices of the firms have an ideological bias to them, which a lot of people believe they do, that's the kind of thing that if we could look at the content moderation enforcement in a detailed way, we would be able to figure out whether this is sort of neutral principles that are having a disparate impact, or whether there is something more nefarious going on. That again, as I said in my opening statement, this is what will change the behavior of the platforms. Right? If they know that their content moderation decisions are going to be transparent and viewed by others, then they will make decisions in a different way immediately.

Chair COONS. Thank you. Mr. Silverman, if I might. I think it's important for people to understand tangibly how transparency of the kind that CrowdTangle as a tool created, and how that could possibly benefit society.

Could you just give us a few concrete examples of how greater transparency might benefit society? I think Mr. Harper appropriately raised the question about, you know, harm to privacy being immediate, and the benefits from greater transparency being remote or contingent, I think was the term.

Mr. SILVERMAN. Yes. Absolutely. I'll go through a few examples, and I'll try to focus on the ones that are immediate, and real-time, and you could get fairly quickly if this sort of legislation was passed.

First there are—is one of the challenges with social media is its scale. We've seen through a lot of research as well as some of the leaked documents over the last year, that it is very hard for these platforms to manage the sheer number of communities, dialects, languages, individual nuances of places where they exist and where they're incredibly important. If you give the outside world the ability to also see what is happening with public content, they can play a role in helping with that effort.

One specific example, in the Philippines, this year's Nobel Peace Prize Winner, Maria Ressa, and her news organization, Rappler, for years have used CrowdTangle to help identify coordinated inauthentic networks that were violating the standards—the community standards of Facebook, helping identify them, flag them for Facebook to get removed before the platform would have themselves.

One, is you have the ability to engage not just the platforms, but a much broader swath of society, in helping monitor, debate, and engage with what's happening on those platforms.

A second one is there is a lot of academic research that can be done on public data. There are very privacy-sensitive datasets that you have to build a lot of controls around to deal with in a safe and responsible way. But even—there's also a lot of publicly available data that can empower a lot of research. We have over 1,000

academics and researchers who have used CrowdTangle, and published hundreds of research papers, including in nature, in science, and others looking at this data to inform lawmakers and policy-makers.

I'll give you this one last one is, I think if you talk about simply, like, at a really high level, the idea of a marketplace of ideas, if in any way we want these platforms, which already house so much of our civic and political discourse, to actually be functional marketplace of ideas, where people can engage and debate with them, you can't do it if people can't see what's in the marketplace. And so simply as creating healthy, dynamic places of liberal debate and engagement, one of the just first foundational things you need is to make it easy to see what's happening. We saw over and over, local news outlets, independent journalists, investigative news, using the data that was coming through our system to both cover the platforms themselves, but also simply talk about issues of the day, and report on them to the public.

Chair COONS. Last question to you, if I might, Mr. Silverman. Some would argue that to your point about marketplace of ideas, that the market should just sort it out, and that any regulatory effort by Congress is likely to overreach or pose as profound risks to privacy. You saw in your experience at Facebook, I don't want to put words in your mouth, but that it was in the market interest of a lot of platforms, other platforms, to simply avoid any transparency whatsoever.

Help me understand why you think it is that large social media platforms want to avoid scrutiny through transparency. And why, in your view, if this is the case, we can't just rely on voluntary disclosures, or on the market—commercial market, to solve this problem?

Mr. SILVERMAN. Yes. I think there are a number of things happening. I'm not an economist, so I don't want to out too far above my expertise, but I think there is a reality in which there are not fully diverse, you know, free markets happening in some of these industries. That there are dominant players that have enormous percentage of the market share and are less subject to the whims of, you know, a free, you know, market of users that can pick among a wide variety of choices. One is, I just think there is a reality of the actual nature of the markets in which these companies operate.

Two is, at this point, we have 10-plus years of evidence that some of these companies can do very little, and it doesn't matter. The reality is there are a lot of challenges to doing it inside Facebook, but one of them was certainly the question of, why are we putting ourselves out on a limb when others aren't? I don't see that dynamic changing at the moment, and maybe that's a judgment call, and I could be wrong. But I think there is just too much evidence in the industry right now of too little efforts around transparency relative to the scale and the need out there.

Just to add one last note on this, while also at the same time the executives all talk about how important transparency is, so I think they both acknowledge its importance, but I think the level of efforts across the industry just haven't met the need we have as a country. And so, now, it's time for legislation.

Chair COONS. Thank you, Mr. Silverman. Senator Sasse for 8 minutes.

Senator SASSE. Eight? Wow. That's generous.

[Laughter]

Senator SASSE. That's good. Let me just first underscore Chris' point. Five for five really useful testimony, the stuff you submitted, even if 300 pages, but also all of your verbal comments here have been useful.

Professor Haidt, I want to start with you because there were a few side comments about how unrepresentative our stereotypical sense of the messed-up conversation, public square, digital public square, is compared to maybe the median experience. You didn't, in your opening statement, refer to your Atlantic piece 2 weeks ago. But given how viral that has gone, in this case, in a good way, would you be willing to unpack your four-part typology on who the overrepresented, very online, very angry, loud people are?

Professor HAIDT. Yes. I've spoken with Mark Zuckerberg a couple of times. I've heard the arguments, and I've heard him say, "How could it be wrong to give more people more voice?" That sounds great. If everybody, especially those who have less voice, were all lifted up, that would be great. But in fact, what I argue has been happening, is one social media developed a tool to make it really, really easy to attack people, criticize them, complain. Once it became not about, look at my nice photos of my kids, but can you believe that this person said that? It was as though everybody was given a dart gun, and everybody could shoot whoever they wanted. But most of us don't want to shoot anyone.

The four groups who are doing most of the darting are the extremists on the far-right, the extremists on the far-left, trolls, who are mostly men with personality disorders. They enjoy harassing people and showing off, and Russian intelligence agents.

Social media, especially Twitter, but also Facebook and others, have been an incredible gift to those four groups. The other 80 percent of us lost voice. We're afraid to speak up. We see this among our students in class. It's horrifying. Our students are literally afraid to challenge something because they're afraid someone will record it, someone will talk about it, someone will shame them.

Social media, there was a period when we were incredibly optimistic. A period of techno-democratic optimism when it seemed, in the early 2000s, like this was going to be the best thing for democracy ever. But I believe what we're seeing is James Madison's nightmare where it just promotes factionalism, and fear of speaking up, and it gives us a distorted marketplace. I would love it if Twitter, if Elon Musk could clean it up so that we weren't so afraid to speak, but right now, people are.

Senator SASSE. Really helpful. For folks who haven't seen it or read it, I highly recommend his Atlantic piece 2 weeks ago. It wasn't exactly called the dumbest decade, but it's something like that.

Professor Haidt, can we stay with you a minute on the teenaged girl harm effects that we see? You worked hard in your written testimony to distinguish between social medias—studies that look at social media in particular from those who look at screen time in general. Can you unpack why that distinction matters?

Professor Haidt. Yes. Because, you know, look. When I was a kid, we all watched too much television. It turns out that was a moral panic. Televisions screens, they don't rot your brain. It was hard to link that to bad health outcomes. Many have said the same thing is happening now, and it turns out, when you look at the research on, say, videogame playing, in general, it's not particularly harmful. Now you know, if you play huge amounts, it's different.

The point is, digital technologies, screens are not bad intrinsically. It depends on what you do with them. If a screen promotes social learning and engagement, in a healthy way, between kids who can connect and play together, that's great. That's not harmful. Watching Netflix is not harmful. Watching videos are not harmful.

And so, much of the research has looked at all digital activities, and they say, "Hey, all digital activities for all kids, the correlation is so tiny, it's not even worth worrying about." But what I found over and over again is when someone sends me a meta-analysis this happened on Twitter just this morning. Someone said, "Here's a meta-analysis from 2020, that this proves your thesis." If you look at the meta-analysis, yes. They find nothing when you look at everything. But whenever you zoom in on social media for girls, you almost always find a much bigger correlation up in the range of $r = 0.1$ to 0.2 , which is, clinically, very serious. This is what public health effects are.

We really have to distinguish. Don't get caught up in digital media and screen time. Focus on social media for girls, especially in middle school. For God's sakes, let kids go through puberty first, before we encourage them to live their lives, putting out pictures and asking people to tell them how pretty they are.

Senator Sasse. Really helpful. I would like to ask some more questions about the solution set relative to that problem because, to me, that is one of the biggest problems we face. Our republic is not going to survive and thrive unless we, the people, have a set of habits that recognize our digital consumption habits are things we're going to have to be responsible for. That doesn't mean there are no collective solutions to any of these problems, but fundamentally, most of what we're talking about with digital addiction is going to have to be responded to at the level of individual, and family, and communication, localist, and healthy institutions that figure out ways to put constraints on our own addictions and consumption.

It seems to me that kids are a completely different category. And so, if I weren't out of time, I would ask a number of you who are advocating for this particular piece of legislation to help me understand why we wouldn't really want to be starting by targeting solutions that deal with the teen problem, or with the minors problem. Given that we're going to have vote soon, and we've got other Members waiting, I'll defer it for later. Thanks.

Chair Coons. Thank you, Senator Sasse. Senator Ossoff.

Senator Ossoff. Thank you, Mr. Chairman. Mr. Silverman, what are the implications of Government access to some of these research tools? Are there Fourth Amendment implications? Privacy implications? Surveillance implications?

Mr. SILVERMAN. I might also let some of the other experts on this panel answer some of that.

Senator OSSOFF. Sure.

Mr. SILVERMAN. But what I will say is any answer to transparency shouldn't be a one-size-fits-all approach. There needs to be tiered access, or in my opinion, there should be tiered mechanisms with different access points, with different audiences, designed to serve different purposes.

Each one of the different set of constraints, and just to give you an example, one way I think about it sometimes is a pyramid or a funnel, where at the very top, you can have the most widely accessible forms of transparency. I think about that as reports. Right now, a lot of platforms put out reports on hate speech, or coordinating authentic behavior, etc. That's available to the public. It's privacy safe. As far as I know, there haven't been any issues raised about Fourth Amendment or First Amendment about it.

As you go down the funnel into more sensitive datasets, with smaller audiences, I think some of those issues get much more prevalent. The idea of having a tiered system would ideally give you a way to address each of those in safe and responsible ways.

But I'll also say there are real issues, and I think ones that also private companies shouldn't be trying to figure out. There's an argument for why Government should be looking at those tradeoffs and figure out a solution.

Senator OSSOFF. Anyone else want to weigh in on the Fourth Amendment or privacy aspects? Concerns that are raised by Government access to these transparency or research tools?

Mr. HARPER. I will try to just briefly. As I detailed somewhat in my written testimony, certainly the PATA legislation, broadly written as it is, would have Fourth Amendment and privacy considerations. The argument I make is that the written materials, the privacy policies and terms of service that platforms put forth, are contracts that allocate that personal information as data. The right to possession is often with the platform. The right to exclude others, which is privacy protection, is with the consumer, subject to narrow exceptions that I think are generally appropriate.

Taking that away, ladling that out for researchers or for any other purpose, would be taking of property from the business, taking of property from the individual. It would be taking the papers and effects, in Fourth Amendment terms, of those people.

The Supreme Court, had some—there's some whiffs of heading that direction. The *Riley* case referred to as digital materialism and the phone as a person's effects. That signifies that it's something owned by the individual. I think that's true whether it's on your phone or whether it's housed for you by a service provider.

Senator OSSOFF. If there were to be enacted transparency requirements for these platforms, would it be sensible that there be transparency requirements for Government access of those transparency tools?

Mr. HARPER. First, limitations. I think the legislation should specify certain categories, perhaps, that should not be available. Certain reasons. Again, the PATA legislation, a discussion draft is very broad, but it gives to the NSF and the FTC the ability to de-

cide what data and what for, and that's far too broad. Congress should actually be the policymaker on those questions.

First, limitations. Then certainly, transparency if the Government accesses that data, either through the NSF/FTC program, or from the researchers themselves. I think, if not entirely barred from access, there should be transparency, if given access that way.

Senator OSSOFF. Professor Haidt, I want to invite you to elaborate on some of what you shared with Senator Sasse with respect to the impact on public discourse and political discourse of how these platforms are functioning. I'm not sure if your research has included this specifically. If not, I invite you to speculate in public about the impact on elite opinion, the opinions of policymakers, and those who staff them, and the activists who are most vocal in advocacy. And then ask you what solutions you're proposing, please.

Professor HAIDT. Thank you, Senator Ossoff. I think that the effect on the elites is extraordinary and is overwhelmingly bad. Many people will say, "Twitter's not that important because, you know, 80 percent of Americans are not even on it, so who cares?" Almost all journalists are on it. If Senators and Congresspeople aren't on it, their staff certainly is, and they're very, very responsive.

We want our leaders, we want our representatives, to be responsive to all of these constituents and to the broader country. But now that they're all on Twitter, they're responsive to the most loud, vocal, angry people on it, so it takes them away from their duty. I would say that representatives who pay a lot of attention to social media are, in a sense, violating their fiduciary duties to the country. I understand why they're doing it. We're all doing it.

Of course, journalists, my God, think about how many stories on the news are about something someone said on Twitter. You know, right-wing ecosystem is much more dependent on cable TV, but even that, they get the stories from Twitter. So they know exactly what the most angering story is going to be.

So, don't listen to anyone who says, "Only a small percentage of people are on it." The influence on those people, then, goes out through many other channels to affect the entire country. We can't have a deliberative democracy if we're not able to deliberate.

I would say that social media has given us an environment which we're sucked into fighting over trivia. We don't deliberate.

Senator OSSOFF. Solutions?

Professor HAIDT. So the solutions, there are a number that are crucial for making social media less toxic. The most important thing is, how can we make it so, you know, of course the extremes are always going to have more voice. They care more. They're more passionate. The middle is always going to have less. Fine. But what happened about 2012, 2014, was the extremes got so amplified, along with the trolls, and the middle went down.

How can we undo that? The most important thing is please stop talking about content moderation. I am so sick of it. What we learned from Frances Hangen, it doesn't actually even matter all that much, whether they get a little bit more or a little bit less. Look at the architecture. That's what changed. That's where the solution lies.

The most important thing is verifying identities. Not that you have to post with your real name, but just as you can't go to a bank

and give them a bag of money and say, “Open an account,” banks have to know your customer laws. Systemically significant platforms that effect the health of our country should be like banks. Not that they’re going to tell you what you can say and can’t say, but they’re going to say, “In order to speak on this platform that has Section 230 protection. We get Section 230 protection, we have a duty to at least verify that you’re a human being, that you’re old enough to be using the platform, we have to be getting to do some age gating and I think also verifying that you’re in a particular country, because we’ll have different rules in different countries. If we do those three things, that would wipe out most of the bots. It would make us less afraid to speak. It would elevate the center and quiet the extremes.

That’s one, but there are many others. Architectural changes. Don’t focus on content moderation.

Senator OSSOFF. Professor Haidt, I’m way over time. I just want to ask you if you got a 15-second response here. How do you respond to folks who point to, for example, the role that anonymous pamphleteering played at various points in our history? Or the capacity of whistleblowers, or those who possess sensitive information to disclose such information and not putting themselves at risk. How does that conflict with what you just suggested, if at all? And that—that’ll be my last question. Thank you.

Professor HAIDT. Sure. The spread of information has always been an issue in democracies. All the things that are going on now, most of them have a precedent. All of these things that used to happen, they didn’t make us afraid of each other. They didn’t make us afraid to speak up in class. This is something new. This is changing the social dynamics.

Don’t just focus on information and false information. Focus on the fear of speaking up. That is what is making our institutions structurally stupid.

Senator PADILLA [presiding]. Thank you, Senator Ossoff. In Senator Coons’ absence, I’m presiding for the time being and will proceed with my questions by recognizing the next Member. Let me just begin by thanking Senator Coons for holding this hearing on platform transparency, and to all the witnesses for exceptionally detailed testimony.

You know, transparency has been a key piece of the debate over the responsibilities of technology companies and the impact their services have on our democracy, and the welfare of our loved ones and our neighbors.

As one of the few Senators with an engineering background, I believe that policymaking is at its best when we’re also armed with research and data. To that end, I support the calls to enhance platform transparency to better serve the public, users of these services, the company themselves, and lawmakers. We have an important opportunity for real productive and effective policymaking.

Before I jump into my first question, I also want to note that I have the honor of representing the State of California, home to more innovators, and executives, and investors in technology than any other State in the Nation. Also, home to more consumers of technology and users of platforms than any other State in the Na-

tion. And of course, more employees in this sector, than any State in the Nation.

And so, my first three questions are a little rapid-fire. Mr. Silverman, what State you from?

Mr. SILVERMAN. California.

Senator PADILLA. Professor Persily, what State are you from?

Professor PERSILY. California.

Senator PADILLA. Professor Keller, what State are you from?

Professor KELLER. California.

Senator PADILLA. No disrespect to the other witnesses.

[Laughter.]

Senator PADILLA. I just wanted to drive home the point California plays a huge role in this discussion and in the problem solving as well, from all angles.

Advocates are routinely highlighting the failure of technology companies to moderate content in non-English languages. As Frances Hangen testified at a previous hearing, 87 percent of all spending combatting misinformation on Facebook is spent on English language content, but only 9 percent of Facebook users are English speakers. That's important data. Other platforms likely have similar disparities, but they haven't publicly disclosed similar information, and I certainly would love to see that data.

Professor Keller, in your testimony, you shared that the EU's Digital Service Act requires public transparency reporting around the number of content moderators platforms employ and what their linguistic expertise is. Do you think similar transparency reporting should be considered in the United States?

Professor KELLER. I agree with you that the language issue is incredibly important. I think one of the most important disclosures from my former client, Frances Hangen, you know, was that not only in languages that don't have as many speakers is the content moderation not as good, but also they don't build machine learning systems that are as good as a result. So the problem is just compounded.

I do think that attention to additional languages is incredibly important. I mean, unfortunately, it's part of what makes of measures of things like prevalence so expensive because it means that you're deploying people in many languages, who need many cultural contexts to try to extrapolate how much content exists across the platform. But yes, I am in reporting that you described.

Senator PADILLA. Just briefly, is there any other types of information or data that would be helpful in addressing this or other disparities that concern you?

Professor KELLER. One of the most important things is to see the actual content that platforms took down, or left up, or demoted. You know, if researchers can't see that, then the platforms are grading their own homework. The researchers can't see if there's a pattern of bias, or if they're making mistakes, or whatever.

This collides with the privacy issues that I identified in my testimony for platforms like Facebook. But certainly, for publicly-shared content, you know, where the person who posted, it hasn't tried to take it down. Having an opportunity for third parties to look at what's actually going on, in multiple languages, you know, from multiple cultural contexts, is really important.

Senator PADILLA. Let alone liability. It further speaks to the complexity of the policy here. On a separate note, when legislating on technology-related issues, I think it's important, and I raised this in the Full Committee previously, important to not enable or incent politically ambitious Government officials with legal authorities who may use our efforts to undermine the ability of platforms to limit the spread of hate speech and election disinformation, just as two examples.

Question for Professor Keller again. In your testimony, you cited the Texas attorney general's ongoing dispute with Twitter as an example of States trying to influence online speech. As Congress considers regulating the conduct of tech companies with respect to transparency and competition, what should we know about the battle over online speech regulation? And what's taking place in the States?

Professor KELLER. Yes. I think it's really important to appreciate the rash of cases out there, litigation, and State laws, some of which have passed, that have the goal of compelling platforms to carry content that the platforms don't want to, that violates the platforms' rules. This includes, you know, white nationalists saying that they have a right to post white nationalist content on Twitter. You know, and there have been over 70 of these cases. The laws that were passed in Texas and Florida both create these obligations to carry content that violates the platforms' rules.

I'm sympathetic in a way. Like, these are the public forums of today. I understand why people are very concerned about being excluded if they are being excluded. But creating a mechanism for government actors to effectively strong-arm platforms about their policies, which I think is what is going on with the Texas AG investigation, is quite dangerous.

I think this is something to worry about with some competition bills pending that are otherwise, I think, really good ideas. I'm sorry that Senator Klobuchar isn't here to hear me talk about her bill, but you know, the 95 percent are about saying platforms shouldn't self-preference and promote their own properties over their competitors. And then, both her bill and Senator Blumenthal's bill, and he's not here either, both have just a couple of sentences that permit a different category of lawsuit. A lawsuit that's Breitbart saying they should be treated like the Wall Street Journal, for example. I think it's a very serious change in the law, if that comes into effect.

Senator PADILLA. Thank you. Speaking of Texas, Senator Cruz.

Senator CRUZ. Thank you, Mr. Chairman. The single biggest threat to free speech in this country, in my judgment, is the power of Big Tech. A handful of Silicon Valley billionaires who have arrogated to themselves complete monopoly power over the public discourse. Professor Keller just referred to these social media sites as the public square, and that is very accurate. It is how we speak with each other. Big Tech has gotten more and more brazen in its abuse of that power.

This is a hearing on transparency for Big Tech. I would be in support of almost anything imaginable to increase transparency for Big Tech. The bill being discussed here is a fairly modest step that gives access to some academic researchers. I suppose that would be

fine. It's not clear to me why a professor at Harvard or Stanford should have some special access that Joe Q Citizen should not. But when it comes to transparency, the people have a right to know. But to the extent academic research marginally increases the ability of the people to know what's going on, I imagine that's a positive step.

The lack of transparency is not an accident. It is a deliberate feature of how Big Tech has set up its systems. To all of the witnesses here today, the 2016 elections. Does anyone know how many posts from Republican candidates for office were blocked? Does anyone know how many posts from Democrat candidates for office were blocked? How about the 2018 election? 2020 election? Does anyone know the average—average ad rate charged by Google or by Facebook to Democratic candidates for office? Does anyone know the average ad rate charged by Google or Facebook for Republican candidates for office?

Nobody knows. I don't know. The Chairman doesn't know. I'll tell you, Mark Zuckerberg has sat at that table. I have asked him that question. I've asked the CEO of Google those questions. I've asked them those questions in writing, and they hire teams of lawyers to write letters back that say, in every way possible, pound sand. We refuse to tell you. By the way, trust us. We're not censoring. We're just not going to tell you.

During the Trump administration, I begged the Department of Justice, if they did nothing else on Big Tech censorship, to use the subpoena authority of DOJ to get answers to basic questions on transparency. I think there were multiple people in the administration who wanted to do that, but they did not get that accomplished.

Few things illustrate the abuse of power of Big Tech over free speech better than the reaction, in the last 2 weeks, to Elon Musk announcing that he's buying Twitter. I find it quite remarkable. I think Elon Musk's buying Twitter is, without exaggeration, the most significant development in favor of free speech in decades.

I also find it astonishing the reaction of much of the corporate media in the left to Elon Musk buying Twitter and, oh my God, suddenly conservatives being allowed to speak, and it is truly Armageddon. It's cats and dogs living together. It is the worst imaginable. Watching the public histrionics of the left, if their opponents are not silenced is amazing.

By the way, Elon Musk, the last I've checked, is not some right-wing character. He's a lifelong Democrat who voted for Barack Obama twice. This is the scary specter because he's dared stand up and say, "You know, we'll allow free speech. We'll allow speech I disagree with."

Look. I'll give you one data point. I asked how many were blocked. Nobody knew. I could ask how many were shadow banned. No one would know because they don't tell you. But I'll give you one data point from my own Twitter page. I am active on Twitter. I spend a lot of time on social media. Twitter accepted Elon Musk's offer to purchase on April 25th. All right. On April 22, my Twitter account gained 1,488 new followers. On April 23, it gained 1,526 new followers. On April 24th, it gained on 1,486 new followers. On April 25th, it gained 1,214 followers. Going back, I was pretty consistent gaining 1,000 to 2,000 a day.

Twitter accepts Elon Musk's offer to purchase them. The next day, April 26th. Mr. Chairman, I would ask you how many new followers do you think I gained the next day?

Chair COONS [presiding]. More than 1,000.

[Laughter.]

Senator CRUZ. You would be correct. The next day, I gained 51,405. The next day, April 27th, I gained 61,261. The next day, April 28th, I gained 70,584. In the week and a half since Elon Musk purchased Twitter, my Twitter followers went from 4.8 million to 5.1 million. Conservatives all across the country have reported numbers like that, have put up numbers like that, and it is obvious. Someone flipped a switch. The Governors they had on that said "silence conservatives" were flipped off. That is the only rational explanation from going from 1,000 to 70,000 the day after he bought it. I'll just point out, he hasn't even taken it over yet. This is just the in terrorem effect of some engineers who, I imagine, are running the document shredders like crazy going, "Crap. They're going to find out what we're doing. Turn the stuff off."

That activity illustrates the need for transparency profoundly, and I hope Congress does something about it.

Chair COONS. Thank you to my colleague from Texas. You, I think, highlight the many ways in which, whether it's from the right or from the left, there are lots of questions about how these platforms operate, how they censor, how they reinforce, how they amplify. I am tempted to ask whether any of you have an alternative suggestion for exactly why the Senator's Twitter followers may dwarf mine in number and scope. A question, perhaps, of interest really only to me, or maybe my colleague from Texas. Mr. Harper, if you'd like to offer—

Senator CRUZ. I follow you.

[Laughter.]

Chair COONS. He does follow me, which I appreciate. One of the very few. My Twitter followers are infinitesimal.

Mr. HARPER. If it's not too late, I wanted to ask Senator Cruz to retweet me. I'm @ Jim_Harper.

[Laughter.]

Chair COONS. Mr. Harper, if you'd like to speak to that, then I have a second round of questions. My understanding is Senator Blackburn is on her way. Are there other Members on their way? Because relatively soon, I am going to have to close the hearing out and go vote the second time. Mr. Harper, if you would, to the intriguing characterization the Senator from Texas made about the unavoidable conclusion one must reach about what is happening at Twitter.

Mr. HARPER. I think we know less than that about how things work in those companies and what occurred in the days that the Musk takeover was reported. Let me say, though, thematically, both his question/testimony and a lot of what we've discussed here, for me, are speech topics. We're talking about what we want our speech in our country to go like, how we want it to go.

This, by the brusque language of the First Amendment, is not the place where that stuff is supposed to be decided. Again, I don't think my written testimony was the strongest on First Amendment issues, and there's a lot there to consider. But I'm sorry to say it,

this body is largely disqualified from regulating speech in the country, and that's for the good for different reasons.

Chair COONS. No. I don't think you should hesitate to say that. I think that is something we can all agree on. This was simply a follow-on to Senator Cruz's questioning.

I'll now yield to Senator Blackburn. She, I think, will be the last of our first round of questioners. Then Senator Sasse and I may have a second round. Senator Blackburn.

Senator BLACKBURN. Thank you, Mr. Chairman. I want to thank each of you for being here. Over at the Commerce Committee, Senator Blumenthal and I have held five hearings this year on Big Tech and the effects that it has on the public writ large, and also on children.

Professor Haidt, I want to come to you with a question, if I may. Let's see, I'm hoping that he is still on—

Professor HAIDT. Yes. I'm here.

Senator BLACKBURN. Okay. Great. As long as you're still there online. Thank you for your opening statement. I have a question for you pertaining to the Kids Online Safety Act that Senator Blumenthal and I have filed. We have a provision in there that would allow independent researchers access to the data that—to these two Big Tech platforms, into the data, how they are holding that data, how they're utilizing, crunching that data, when it comes to harms to minors. What I'd like for you to do, for just a moment, is talk about in your research and the work that you are doing with research, and parents, and teachers, physicians, policymakers, what are you finding, when it comes to kids 18 years of age and under as to the impacts and the experience that they have on these social media platforms?

Professor HAIDT. Thank you for that question. The fundamental reality, the thing we have to keep our eye on, is that using social media is not like consuming sugar. A lot of the research has looked at, you know, if you consume a lot, do you get more sick? If you consume a little, do you get a little sick? But if we look at it from the kids' point of view, what we have to see is that children have always wanted to play with each other, and talk to each other, and do things with each other. It's when, around 2011, plus or minus, when they all got online, they spent so many hours online performing for each other, they don't have much time to actually connect and play. Now when they're actually online, sometimes they say it's fun. Sometimes they say it's not. That data is mixed. The overall impact on them is clearly negative, and this has been overwhelmingly consistent.

I gave a talk at my old high school, Scarsdale High School, just before the pandemic, and all of the teachers are like, "We can't get through to the kids. They're not paying attention. This is a disaster." By the time they come in already, a lot of them are depressed and fragile.

I gave a talk at my middle school in Scarsdale, and I spoke to the principal there, and the teachers there. They said the same thing. In fact, they even said by the time they come to us in sixth grade, they're already addicted to their devices, many are fragile, many of them are depressed and anxious.

What we're hearing consistently from all who work with kids is this is messing them up, and we didn't give——

Senator BLACKBURN. Okay.

Professor HAIDT. We don't want this to be happening. I think it's been terrible from all reports. I don't know anybody who's happy that our kids are now spending, you know, 4 to 10 hours online on social media every day.

Senator BLACKBURN. Yes. We are hearing some of the same things, and it's why we have put the provision in there, in the bill, that would allow this research.

Ms. Keller, it's good to see you again. I want to talk with you about privacy because, as you know, the EU has moved forward with a Digital Services Act and a Digital Marketing Act. One is more closely akin to our 230, the services. But their Marketing Act does deal with privacy.

We have yet to address this issue in the U.S., even though some of us are hard at work on it. I would like for you to touch on why we need to make certain that we have a consumer privacy bill that exercises Federal preemption.

Professor KELLER. I'm an ex-privacy lawyer. It's good to see you again, too.

Senator BLACKBURN. Yes.

Professor KELLER. I'm an ex-privacy lawyer, and most of what I've worked on is the GDPR. The General Data Protection Regulation in the EU, and it gives them a baseline, to start with, of how privacy is supposed to work. Then you can build transparency on top of it and have some starting point rules, and some mechanics for resolving the new questions that arise, you know, when it comes to platform transparency. The Digital Services Act, as I mentioned in my testimony, it has multiple transparency provisions. It has almost all of the provisions that are in PATA, although it does not have the scraping provision, which is the sort of like democratic scrappy kind of research. That one's not in the DSA.

In particular, the researcher access, so that analogue of the first four or sections of PATA, which is in Article 31 of the DSA. Because the GDPR is there, and because they're able to convene experts, and this is happening right now. There should be a code out by the end of the month, trying to say how this is going to work with privacy.

You guys are in a much more difficult position because you don't have that baseline. And so, the lack of Federal privacy legislation to start from leaves you having to answer questions that shouldn't be your job to answer it.

Senator BLACKBURN. Thank you. I appreciate that. We need to get to that starting point. Thank you, Mr. Chairman.

Chair COONS. Thank you, Senator Blackburn. Senator Sasse, any closing question you'd like to ask before you have to go?

Senator SASSE. No. Thank you, again, to all of the witnesses, and to not just you, but your team for organizing this. It's been instructive, and I'm sure we'll have follow-ups. Thanks.

Chair COONS. If I might, I'm going to ask a couple of more questions until I get told I have to go back and vote again. Professor Keller, to the point that Senator Blackburn was raising, help me better pull apart the tensions, competitive impacts, privacy con-

cerns, and how you think progress, that's how I view it, in your—the foundation of GDPR and the potential. We don't yet have the full text for Digital Services Act, but where do you think Europe is going? What should we learn from European regulatory legislative efforts in terms of the balance we might strike, both around individual privacy, and privacy rights in the digital domain, but also competitive consequents, competitive concerns? Do you think PATA strikes the right balance? Do you think there are other ways in which we might make sure that we are protecting privacy and companies' interests in competitive concerns?

Professor KELLER. Yes. There was a lot in there. Please.

Chair COONS. Yes. Take your time, unpack, and then I'm going to invite anybody else who wants to respond to that, as I'm sure Mr. Harper will.

Professor KELLER. Yes. There are things I really like about the DSA as a regulatory approach. I actually had an op-ed in *The Hill* a couple of years ago saying, "Congress can learn things from how Europe approached the equivalent of 230 issues."

Chair COONS. Your editorial saying, "We hope that Congress can learn things."

Professor KELLER. I was more polite than that. You know, there are great things about it. I do think that it gets the balance of competition and other values a little wrong. If you want to get really in the weeds, I have a blog post on that on something *The Verfassungsblog*, which is a German constitutional law blog. It's awesome. You know, it goes into how effectively I think the DSA is sacrificing competition goals in the name of content regulation goals, or you know, speech control goals by putting lots and lots of mechanical burdens even on very small platforms, you know, that I think are just, you know, disproportionate. It'll make it harder for them to grow up and compete with the bigger platforms.

Chair COONS. One of the concerns you've raised in our conversations about PATA is making sure that we're not writing rules that are unduly burdensome for smaller platforms. If you'd make a brief comment on that, I'd appreciate it.

Professor KELLER. Yes. I think that's right. I mean, so PATA has 25 million monthly active users and up as its size range. I put in an exhibit that I can't swear it's right because nobody really knows these numbers, but it at least tries to get at a question of which platforms is this talking about? You know, and a lot of them, I think, are not the kinds of platforms that people have in mind when they're asking for this transparency.

I should say, also in transparency, I do some consulting for Pinterest, and Pinterest is somewhere on that list. But you know, think of a platform like GlassDoor, which is people talking about their employers. You know, that doesn't have the democratic discussion consequences of a Twitter or a Facebook. And so the justification for wanting transparency is lower, and their capability of carrying that burden is also lower.

Chair COONS. Small-D democratic.

Professor KELLER. Small-D democratic.

Chair COONS. If I may, I'm going to jump to Mr. Silverman. I'm going to keep going until I get a text saying, "You got to leave now, Senator." PATA, the Platform Accountability and Transparency

Act, creates a requirement platforms provide ongoing disclosure of information of the type that has fewer privacy implications, public-facing content, typically viral public-facing content, platform advertising practices. How would expanding disclosure of that kind of information, that I would argue has a lower privacy risk, actually help the public better understand how platforms are impacting on-line discourse?

Mr. SILVERMAN. Yes. Thank you for that question. I'll start off by saying that I agree with your assessment, that there are types of content on these platforms that have greater privacy risks, and there are also types of content that have less. We had a very stringent set of lawyers and policy folks at Facebook, but the work we were able to do was able to be blessed from their perspective, in terms of whether it was privacy-safe or not.

There is a lot of content on these platforms that has very minimal privacy risk. One version of that that I think PATA tries to capture, and I think is a really promising place to move, is they give out content that comes from particularly public, or in some cases what some of us may call reasonably public accounts. If you think about the President of the United States or, you know, a major media outlet that uses an account in a very public way, has millions of followers, and uses it for their official business, can you, in some ways, treat that as a type of content where there are less privacy implications, and you could make publicly available to a wide swath of the public.

When you do that, there is a lot of discourse that is shaped by influential large accounts on these platforms. Even just providing a real-time window into those accounts and that content is enormously valuable to being able to see an important part of what's happening on these platforms.

Chair COONS. Mr. Harper, you've raised some concerns about privacy in particular. If I understood your opening testimony, it was essentially that the balance of interests, there's not enough public good to be accomplished here to outweigh the risks to privacy. Could you see some reasonableness to Mr. Silverman's point, that there may be some accounts that are so clearly geared toward large-scale public communication where the privacy risks of offering, sort of, an under-the-hood look at those accounts are less, and arguably worth, that tradeoff?

Mr. HARPER. Yes. I think there are a lots of ways probably to slice and dice what information is made available to researchers or made available publicly. Obviously, information that is not personally identifiable doesn't have privacy risks. It has risks that will be reidentified, and that's important to consider.

I think that's an interesting idea, the accounts that are so public that we don't treat their behavior as private. It might be appropriate to modify the terms of service so that if you are a public figure, for example, you don't get the same privacy that a private citizen does. I, you know, can't think through here on my feet exactly all of the manifest of issues.

Chair COONS. I understand.

Mr. HARPER. But certainly, there are ways to limit the privacy consequences of this hearing. My point, which I think again, is that the wholesale form that PATA allows for threatens privacy because

it could be lots of communications. I appreciate Professor Keller joining me over here on the skunk side of the garden party to highlight those kinds of concerns.

If I may just briefly, in the negative 2 minutes you have left, I see things—so we line up in interesting ways, of course. But I sort of see things, a phase shift, differently on this question of GDPR, for example. It's an outgrowth of the Fair Information Practices, which arguably arise from the Privacy Study Committee that the Health, Education, and Welfare Department put together in 1971. I'm saying 1971, as I am unsure of what year it was. It was back around then.

Ever since the FIPs came into existence, they have been sort of the intellectual way we figure out what privacy protections should be. They were obviously more firmly adopted in Europe. They're here in the Privacy Act, for example, of 1974. But they were in adopted in Europe because of the civil law tradition in Europe, which is an intellectual tradition. The smart, thoughtful people get together and figure out what the rules should be.

Common law and civil law aren't entirely separate from one another. The categories aren't clean. But the common law tradition of England and the United States is a little more loosey-goosey.

Really, in the privacy area, you see distinctions culturally between Europe and the United States, where in Europe, privacy is really more of a dignity value so that everybody gets the same treatment as the princes, and kings, and queens have gotten. In the U.S., it's more of a liberty value, that is keeping King George out of my house. We have common law privacy protections. A contract is common law. Property is common law, but also the privacy torts here in the United States.

I think when it comes to getting data out of these companies, GDPR is a significant disincentive. Mr. Silverman talked about having to go through the lawyers because of the extreme pressure they're under on the privacy side. If your rule is do no harm, you've got a little more leeway to act than if your rule is we've got this legislation, and we've got this regulator in the FTC who's over our shoulder.

In my written testimony, I talk more about the common law, and I think it's a better way to get more innovation and to release a little bit of pressure so that there can be a more give and take that allows researchers access to data.

Chair COONS. Thank you, Mr. Harper. Professor Persily, if I might, because I'm going to ask you one last question, Professor Haidt one last question, and then go off to the joy that is legislating with my colleagues.

Platform Accountability and Transparency Act, sorry to keep coming back to it, but you know, part of my goal here today was to take both critical and complimentary input, and then further refine it. It requires that platforms turn over datasets to researchers upon review and approval by the NSF. Some of this data really could be sensitive in ways that I'm concerned about, and I'd be interested in your explanation, your insights, into how the FTC could best work to ensure that user privacy isn't compromised in datasets disclosed to researchers, and best could be effective as an overseer

or policing function of how that data is used going forward, in ways to be most protective of individual privacy.

Professor PERSILY. Thank you for that. I think PATA does the kind of tiered disclosure that Brandon was talking about, which is that for the sections that look at algorithms, the content, and advertising, right, that is going to be more publicly available. We'll have aggregated reports.

The same may be true for some of this, what we're going to call, sensitive data here that sometimes aggregated information is going to be the way that it would be given to researchers. No personally identifiable information should be given to researchers. I think the FTC would make that clear.

Researchers are not interested in going and looking at individual accounts. Right? We want to know sort of groups of people and what they are going to be sharing and engaging with. And so, I think whether it's through technology as a differential privacy, other kinds of anonymization techniques, this is something that we do all the time, and this is something that the FTC, which also, as we know, has fined Facebook \$5 billion for privacy violations, right, is the right institution to oversee this.

We do need to have privacy baked into this, both in the legislation and the regulations that would come out of it, but this is a balance that can be struck. We need to be clear, you know, and I think whether it's heaping more privacy protections into the bill itself or just making clear through the iterative process of the Agency that no, there should not be any individual whose privacy is compromised by this, but we need to make sure that, you know, someone other than the data scientists at the firm are able to make the kind of inferences that those on the inside are able to do.

Chair COONS. Thank you. I think it was framed really well, I think it was by you, that we need to be able to have the rest of the world have insights as comparable to those who are actually designing, and operating, and running, and making profit from these firms rather than our current situation, where they know virtually everything and we know virtually nothing.

Professor Haidt, if I might invite you to make a closing comment if there's concerns, or issues, or questions that have been raised by the testimony so far, I'd welcome. My question to you is why is this important? Why act now? Why not simply wait and let the market work itself out? You're muted.

Professor HAITT. Okay. Thank you. Thank you, Senator Coons. First, I want to apologize to Senator Ossoff. I misunderstood his question. He was asking when I recommended identity authentication, is this going to put whistleblowers at risk. The answer is no, because identity authentication doesn't mean you post under your real name. You just prove that you are somebody who you say you are to a third party, ideally a nonprofit or something that would be protected. Even if you were afraid of that, you could still just put up an anonymous blog anywhere you want on the internet, and just tell a journalist, "Hey, here's the whistleblowing stuff on this blog." Identity authentication would reduce a lot of the garbage and the nastiness. Still, there's plenty ways to be able to explore complete security.

With regards to your question about any sort of closing statement, and especially why now, in the graphs in my submitted testimony, I show that there are hockey stick-type graphs. That is a long, straight line, and then it goes up, and up, and up. I deliberately focused my analysis up to 2019, before COVID because I didn't want to be confused with what COVID has done. Everything I have said is so much worse now that COVID has basically taken kids and given them less free play outside and more time on their devices.

The problem keeps getting more and more serious. It's now to the point where something on the order of a quarter of our girls seem to have depressive disorder or severe anxiety. And it keeps going up, and up, and up. We should have acted—we should have acted 10 years ago. Well the data was only really clear about 6 years ago. We should have acted then. We didn't, and I think we have to act now.

Even if you're not convinced that I'm right about causation, we don't have the data. We're trying—as my NYU colleague, Josh Tucker, put it, researchers are working with one hand tied behind our back. We have to do secondary studies and try to look at shadows, whereas they've got the data. They know exactly what the kids are consuming, and they know how happy the kid is. They can code their content. Almost all of the data is there. We can't get to it, so we're guessing. We're flying blind. This really needs to change, and I hope that Congress can help us here.

Chair COONS. I'd like to express my thanks to all of the witnesses who have appeared today. I'm also grateful to the Members who attended and asked thoughtful questions. I'm particularly appreciative to Ranking Member Sasse for being a great partner on this Subcommittee and allowing us to hold this hearing.

It's reinforced my view that there is much more that platforms can and must do to be more transparent about how their products and services actually affect each of us, our families, our community, our society, our democracy. I believe that both the public and policymakers need better information if we're going to understand and act on the impact of social media and find better solutions that will allow us to take advantage of all that social media has to offer, while limiting the harms that it creates or even exacerbates.

It's clear we've got a lot more work to do, and I look forward to working with my colleagues and with each of you. I, really, again, deeply appreciate your constructive comment and input today.

Members of this Committee can submit questions for the record for the witnesses. They are due by 5 p.m., 1 week from today, thus on May 11th. I want to thank our witnesses again for participating in this compelling and engaging hearing.

With that, today's hearing is adjourned.

[Whereupon, at 3:49 p.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

**Teen Mental Health Is Plummeting, and
Social Media is a Major Contributing Cause**

Testimony of Jonathan Haidt

Professor of Ethical Leadership, New York University – Stern School of Business
Before the Senate Judiciary Committee, Subcommittee on Technology, Privacy, and the Law
May 4, 2022

I am a social psychologist who has been studying moral psychology and moral development since 1987. I began to notice something going wrong with the mental health and social behavior of college students around 2014, which led me to collaborate with Greg Lukianoff to write an Atlantic article in 2015 titled [The Coddling of the American mind](#). We expanded our research and published a book with the same title in 2018. Since then I have worked with Jean Twenge (a professor of psychology at San Diego State University, and author of *iGen*) to aggregate the academic research on teen mental health and its relation to social media use in two large collaborative reviews, carried out in Google Docs open to other researchers. It is these two collaborative reviews that form the basis of my testimony today. They can be accessed here:

1) Adolescent mood disorders, self-harm, and suicide rates: A collaborative review
<https://tinyurl.com/TeenMentalHealthReview>

2) Social Media and Mental Health: A Collaborative Review
tinyurl.com/SocialMediaMentalHealthReview

I believe I can be most helpful to this committee by first summarizing the academic literature on the changes that have occurred in teen mental health since 2012, and then spending a bit more time explaining the research linking deteriorating teen mental health to the arrival and widespread adoption of social media, which transformed childhood activity, attention, social relationships, and consciousness in the years between 2009 and 2012. I will conclude with some specific recommendations for policies that I believe would have a substantial and positive impact on the crisis.

In the interest of time, I will focus my remarks on the effects of social media on teen mental health. I am also extremely concerned about the effects of social media on America's political dysfunction, which I have written about in a recent Atlantic article, titled: [Why the past 10](#)

[years of American life have been uniquely stupid](#). My claims in that article are supported by a third open source collaborative review, titled: [Social Media and Political Dysfunction: A Collaborative Review](#). I curate that Google Doc with professor Chris Bail of Duke University, the author of *Breaking the Social Media Prism*.

I will state my case in outline form in this document, with links to relevant sources. I will expand on this outline in my testimony, and I welcome questions and challenges from committee members.

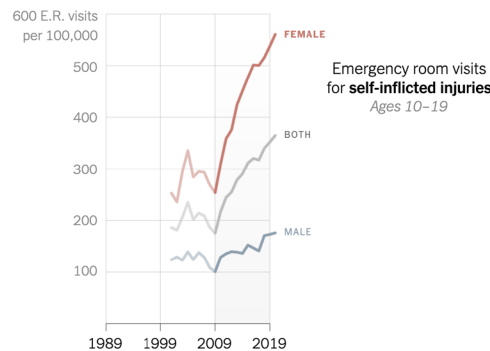
PART 1: THE SPECIFIC, GIGANTIC, SUDDEN, AND INTERNATIONAL MENTAL HEALTH CRISIS

(See the [adolescent mood disorders](#) Google Doc for supporting evidence)

1.1. The crisis is specific to mood disorders – those related to depression and anxiety. It is not a general across-the-board increase in other illnesses.

1.2. The crisis is not a result of changes in the willingness of young people to self-diagnose, nor in the willingness of clinicians to expand terms or over-diagnose. We know this because the same trends occurred, at the same time, and in roughly the same magnitudes, in behavioral manifestations of depression and anxiety, including hospital admissions for self-harm, and completed suicides. Figure 1, below, from a [New York Times article](#) (April 23, 2020), shows just how sharp and sudden the increase has been for hospital admissions for teen girls who had intentionally harmed themselves, mostly by cutting themselves.

Emergency room visits for self-harm by children and adolescents rose sharply over the last decade, particularly among young women.



By The New York Times | Source: Centers for Disease Control and Prevention

Figure 1: Emergency room visits for self harm increased very rapidly among teen girls beginning in 2010

1.3 The crisis came on suddenly, in the early 2010s.

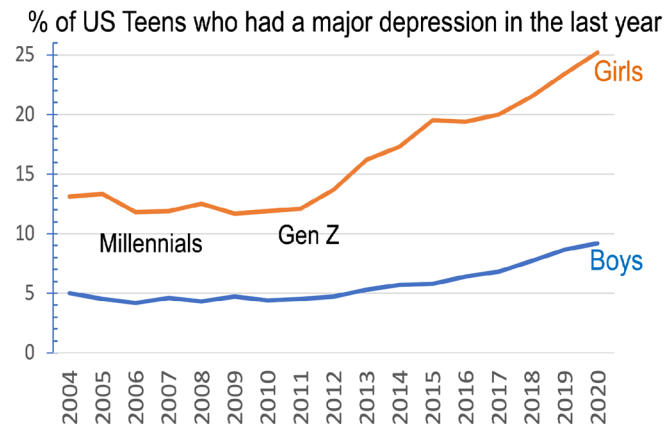
The curves you can see in the Adolescent Mood Disorders Google Doc are not just the continuation of trends already in evidence for the Millennial generation (born 1982 through 2016). They are more like “hockey sticks,” with a long relatively flat period before the early 2010s, and then a sharp upturn or elbow. This is rare in mental health data. It suggests that something changed in the lives of American teens around 2010.

1.4 The increases in mental illness are very large.

When you compare rates in 2009—before most teens were daily users of social media—to 2019—the last full year before Covid made things even worse—the increases are generally between 50% and 150%, depending on the disorder, gender, and subgroup.

1.5 The crisis is gendered.

The collapse of mental health has hit both sexes, and on many measures, boys and girls are up by roughly similar percentages. However there are two important caveats: A) the base rate for mood disorders is always higher for girls than boys, particularly after puberty, which means that a doubling of the rate produces far more additional sick girls than boys, as you can see in Figure 2 below, and B) there are some disorders and age groups for which girls are up far more, especially for self-harm, which is a much more common way of manifesting anxiety in girls than in boys.



Source: U.S. National Survey on Drug Use and Health

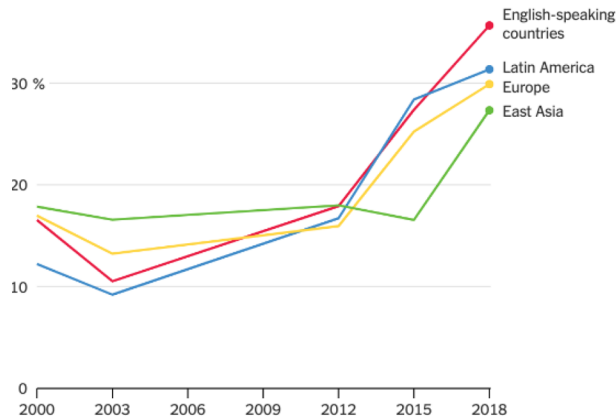
Figure 2: rates of major depression roughly doubled, for boys and for girls, from 2010 to 2020.

1.6 The crisis has hit many countries, not just the USA.

The patterns are nearly identical in the UK and Canada, and the trends are similar though not identical in Australia and New Zealand. We do not yet see signs of similar epidemics in continental Europe or in East Asia, although I have not yet found good data from those regions. Jean Twenge and [analysed the PISA dataset](#) – the one global survey given to adolescents around the world. The survey focuses on educational outcomes, but it contains seven questions related to loneliness at school. Sure enough, we found a sudden increase between 2012 and 2015 in all regions of the world. These patterns indicate that whatever happened to American teens was not uniquely caused by trends and events in the USA (e.g., a sudden fear of school shootings after the Newtown massacre of 2012). The cause is likely to be something that affected teens in many or all regions of the world at the same time. Figure 3 below is drawn from our [New York Times op-ed](#) about our academic essay:

Lonely at School

The share of students reporting high levels of loneliness at school has increased sharply since the early 2010s.



By The New York Times | Note: English-speaking countries include Australia, Canada, Ireland, New Zealand, United Kingdom, United States. Source: "Worldwide increases in adolescent loneliness" by Jean M. Twenge, Jonathan Haidt, et al.

Figure 3. Loneliness at school increased in all regions of the world after 2012.

PART 2: THE EVIDENCE THAT SOCIAL MEDIA IS A SUBSTANTIAL CONTRIBUTOR TO THE CRISIS

(See the [Social Media and Mental Health](#) collaborative review for supporting evidence)

2.1 Correlational studies consistently show a link between heavy social media use and mood disorders, but the size of the relationship is disputed.

See the studies in [section 1.1](#) of the review. Nearly all studies find a correlation, and it is usually curvilinear. That is, moving from no social media use to one or two hours a day is often not associated with an increase in poor mental health, but as usage rises to 3 or 4 hours a day, the increases in mental illness often become quite sharp. You can see this pattern below in two studies, the first from the USA, the second from the UK.

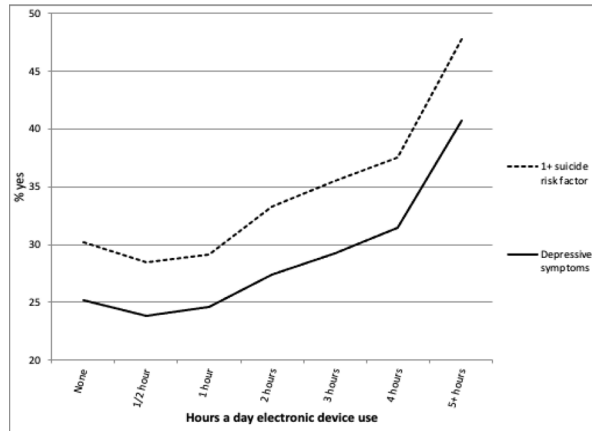


Figure 4: Exposure-response relationship between electronic device use and a) having at least one suicide-related outcome/ risk factor or b) depressive symptoms (feeling sad or hopeless for two weeks or more in a row), U.S. 9–12th graders, Youth Risk Behavior Surveillance Survey (YRBSS), 2009–2015. Taken from: 1.1.3b [Twenge, Joiner, Rogers, & Martin \(2020\)](#).

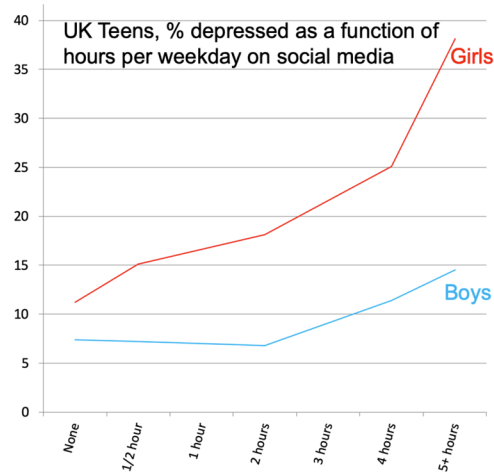


Figure 5. Percent of UK adolescents with “clinically relevant depressive symptoms” by hours per weekday of social media use, including controls. Haidt and Twenge created this graph from the data given in Table 2 of [Kelly, Zilanawala, Booker, & Sacker \(2019\)](#), page 6.

2.2 The correlation is much larger than for “eating potatoes” or “wearing glasses.”

There is one academic publication that is more widely cited than any other in essays that are skeptical of a link between social media use and mental health: [Orben & Przybylski \(2019\)](#), titled: The association between adolescent well-being and digital technology use, published in the journal *Nature Human Behavior*. This study used an advanced statistical technique on three very large data sets in which teens in the US and UK reported their “digital media use” and answered questions related to mental health. Orben and Przybylski report that the average regression coefficient (using social media use to predict positive mental health) is negative but tiny, indicating a level of harmfulness so close to zero that it is roughly the same size as they find (in the same datasets) for the association of mental health with “eating potatoes” or “wearing eyeglasses.” The relationships are equivalent to correlation coefficients less than $r = .05$. The authors conclude that “these effects are too small to warrant policy change.”

How can this finding of a nearly-zero effect size be reconciled with the obviously larger relationships seen in figures 4 and 5? Jean Twenge and I argued in a [published response paper](#) in the same journal that Orben and Przybylski made 6 analytical choices, each one defensible, that collectively ended up reducing the statistical relationship and obscuring an association that is actually equivalent to a correlation coefficient of around $r = .20$. The first issue to note is that the “potatoes” comparison was what they reported for all “digital media use,” not for social media use specifically. Digital media includes all screen based activities, including watching TV or Netflix videos with a sibling, which are not harmful activities. In their own published report, when you zoom in on “social media” only, the relationship is between 2 and 6 times larger than for “digital media.” Also crucial is that Orben and Przybylski lumped together all teens (boys and girls), while many studies have found that the correlations with harm are larger for girls. So even if the association is weak for all kids using all screens, the association is much larger if you zoom in on girls using social media.

2.3 There is an emerging consensus that the correlation is in the ballpark of $r = .10$ to $r = .15$.

Orben and Przybylski obtained an unusually low numbers for the relationship between “digital media use” and mental illness, compared to other published studies. How large is the relationship when we just look at social media? Amy Orben herself conducted a “narrative review” of many other reviews of the academic literature ([Orben, 2020](#)). Her own conclusion is that “The associations between social media use and well-being therefore range from about $r = -0.15$ to $r = -0.10$.” I agree with this assessment, for both sexes combined.

2.4 The correlations are larger for girls.

What would the correlation be if we could just look at girls? Several studies have found that it is substantially larger than for boys. See [Kelly, Zilanawala, Booker, & Sacker \(2019\)](#), [Nesi & Prinstein \(2015\)](#), and [Twenge, J.M. \(2020\)](#). I know of no study that has found a larger relationship for boys. A ballpark figure for the correlation just for girls is roughly $r = .15$ to $r = .22$.

2.5. The effect size is even larger for girls going through puberty.

A very recent study—[Orben, Przybylski, Blakemore, & Kievit \(2022\)](#)—found that the link between social media use and mental illness varies by age and sex. For girls, it is largest between the ages of 11 and 13 -- the years when they are in early puberty. For boys the most sensitive age is later (14-15), consistent with the fact that boys hit puberty later than girls. This means that zooming in on girls and social media is not enough. We must pay special attention to girls going through puberty while on social media. For them, the size of the correlation with poor mental health could be well above $r = .20$. This recent study points us to the urgency of getting social media out of middle schools, at the very least. That is where the harm seems to be greatest.

2.6. Correlations between .15 and .20 are not “small.”

Many researchers learned in graduate school that a correlation coefficient of $r = .5$ and above is a “large” correlation, $r = .3$ and above is a “medium” sized correlation and $r = .10$ and above is a “small” correlation, with $r < .10$ being trivial, not even “small.” But recently, psychologists have noted that these cutoffs make no sense; what counts as large or small varies by domain. The key paper here is [Gotz, Gosling, and Rentfrow \(2020\)](#), Small Effects: The Indispensable Foundation for a Cumulative Psychological Science. The authors note that in the domains of public health and education, many of the things that warrant public expenditure are correlated with outcomes in the ballpark of $r = .05$ to $r = .15$. For example, Gotz et al. note that the correlation of calcium intake and bone mass in pre-menopausal women is $r = .08$, which is enough to recommend that women take calcium supplements. The correlation of [childhood lead exposure and adult IQ](#) is $r = .11$, which is enough to justify a national campaign to remove lead from water supplies. These correlations are *smaller* than the links between mood disorders and social media use for girls. Gotz et al. note that such putatively “small” effects can have a very large impact on public health when we are examining “effects that accumulate over time and at scale”, such as millions of teens spending 20 hours per week, every week for many years, trying to perfect their Instagram profiles while scrolling through the even-more-perfect profiles of other teens.

2.7. The experimental evidence confirms the correlational findings.

All social scientists know that “correlation does not imply causation.” We generally give more weight to experimental studies that randomly assign individuals to a treatment or control condition. Some experiments require participants to reduce or eliminate social media use for a few days or weeks; some experiments randomly assigned participants to spend time on a social media platform (vs. some other activity). [Section 3](#) of the social media collaborative review collects the abstracts of all the experiments we’ve been able to find that were published after 2014. At present, ten of the studies show a statistically significant effect on mental health or happiness, while just four studies failed to find an effect. It must be noted that nearly all of these experiments used college students or older samples; none used middle school students, who are likely to be the most vulnerable to the harms of social media. (Doing experiments with younger teens should be an urgent research priority.)

2.8. The “eyewitness testimony” confirms the academic findings: social media is a culprit.

[Section 4](#) of the Social Media collaborative review collects studies that have directly asked teens what they think is going on. Teens often say that they enjoy social media while they are using it — which is something heroin users are likely to say too. The more important question is whether the teens themselves think that social media is, overall, good for their mental health. The answer is consistently “no.” Facebook’s own internal research, brought out by [Frances Haugen in the Wall Street Journal](#), concluded that “Teens blame Instagram for increases in the rate of anxiety and depression ... This reaction was unprompted and consistent across all groups.”

Insight 34

Young people think social media is the main reason youth mental health is getting worse.

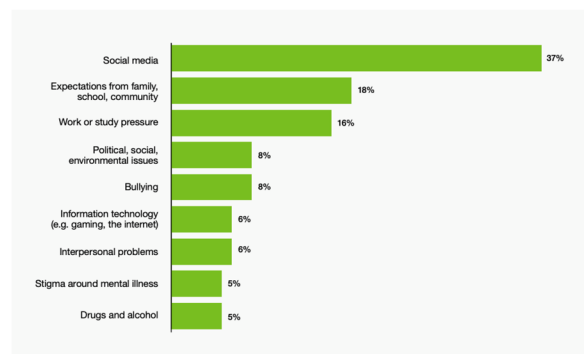


Figure 55.

Reasons for the opinion that the mental health of young people is getting worse

Figure 6: Australian teens believe that social media is the main reason that youth mental health is getting worse. Source: [Headspace National Youth Mental Health Survey \(2018\)](#).

PART 3: WHAT LEGISLATION WOULD BE HELPFUL IN ADDRESSING THE CRISIS?

The United States is experiencing a catastrophic wave of mood disorders (anxiety and depression) and related behaviors (self harm and suicide). The crisis is so severe that the U.S. Surgeon General, Vivek Murthy, recently issued an [Advisory on Youth Mental Health](#).

This crisis did not emerge gradually. There was no sign of it before 2010, but by 2015 it was everywhere, overwhelming mental health centers that catered to teens and college students. The crisis emerged in the exact years when American teens were getting smart phones and becoming daily users of social media platforms such as Instagram. Correlational, experimental, and eye-witness testimony points to social media as a major cause of the crisis. I do not believe that social media is the *only* cause of the crisis, but there is no alternative hypothesis that can explain the suddenness, enormity, and international similarity that I laid out in part 1 of this document. Researchers and spokespeople for the major platforms who tell you that the evidence is “inconclusive” or that the effect sizes are “too small” should be asked directly: “OK, then what do YOU think caused this?”

What should be done? What legislation can Congress pass that might address and reverse America's rolling mental health disaster? My main essay on the effects of social media on teen mental health is a 2021 Atlantic essay titled [The Dangerous Experiment on Teen Girls](#). In that essay I laid out the evidence, as I have in this document, and then I offered three policy suggestions. **The first was that Congress pass the very bill that you are considering today:**

*First, Congress should pass legislation compelling Facebook, Instagram, and all other social-media platforms to allow academic researchers access to their data. One such bill is the **Platform Accountability and Transparency Act**, proposed by the Stanford University researcher Nate Persily.*

My second suggestion was that you consider **updating COPPA**:

Second, Congress should toughen the 1998 Children's Online Privacy Protection Act. An early version of the legislation proposed 16 as the age at which children should legally be allowed to give away their data and their privacy. Unfortunately, e-commerce companies lobbied successfully to have the age of "internet adulthood" set instead at 13. Now, more than two decades later, today's 13-year-olds are not doing well. Federal law is outdated and inadequate. The age should be raised. More power should be given to parents, less to companies.

I strongly believe that Congress must undo the disastrous mistake of setting the age too low and letting the companies off the hook for enforcing even the low age of 13. Puberty and middle school are already so hard, especially for girls. Social media makes it all worse, and that recent study by [Orben, Przybylski, Blakemore, & Kievit](#) shows us that this vulnerable period is when mental health damage is most likely. We do not know if the damage done in middle school is permanent, or if the children will outgrow it if they were to leave the most toxic social media environments. But we can all work together to ensure that middle school children are not on Instagram and other platforms, especially when they are only 11 or 12 years old.

I now believe there is an additional approach that is extremely promising, in part because it is politically very feasible. This is my third suggestion: **to simply pass the [Age Appropriate Design Code](#) that the UK Parliament has already enacted.** The genius of this approach, developed by Beeban Kidron of the House of Lords, is that it recognizes that children are everywhere, on nearly all platforms, including those designed for adults. It specifies the responsibilities of all platforms to provide a suitable environment for children, if they fail to keep children off. The state of California is currently considering implementing the UK's code. The bill recently passed out of a subcommittee on a unanimous and bipartisan vote. The bill, AB 2273, would create the

California Age Appropriate Design Code Act. You can read about the bill [in this essay](#). Of course, a state by state patchwork of bills makes no sense for the Internet. **I strongly urge this committee to consider putting forth a federal version of the same bill.**

My fourth and final suggestion is that **Congress authorize and facilitate research on this topic**. Of course, many researchers are already working on it, but we are working in the dark. We do not have access to the best and most informative data -- the data held closely by the companies themselves. The Platform Accountability and Transparency Act will help researchers gain access. **The Children and Media Research Advancement Act (CAMRA)** which you are currently considering would provide funds to speed up this research. I urge you to enact it.

* * * * *

Surgeon General Murthy wrote in his Advisory: *"Our obligation to act is not just medical—it's moral"* (p. 4). Will the Senate rise to meet this obligation? Can it find the bipartisan will to address the most non-partisan of all issues: the widespread and increasing suffering of America's children?



Statement before the Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law
On Platform Transparency: Understanding the Impact of Social Media

Privacy and Other Challenges for Mandated Internet Platform Disclosure

JIM HARPER

Nonresident Senior Fellow

May 4, 2022

The American Enterprise Institute (AEI) is a nonpartisan, nonprofit, 501(c)(3) educational organization and does not take institutional positions on any issues. The views expressed in this testimony are those of the author.

Chairman Coons, Ranking Member Sasse, and members of the subcommittee:

Thank you for the opportunity to testify before you today. I am Jim Harper, a nonresident senior fellow with the American Enterprise Institute and a senior research scholar at the University of Arizona's James E. Rogers College of Law. For a little over two decades, I have been a policy analyst specializing in the intersection between technology and society. My major area of focus has been privacy, with forays and necessary study in a number of other areas, including transparency, telecommunications, counterterrorism, cryptocurrency, and more.

Executive Summary

There is a great deal of appeal to having greater transparency in all our institutions, including internet platforms. I have some experience with trying to create transparency one place where it lacks: in the US federal government. My experience is that it is hard to create usable transparency.

The mode adopted in legislation such as the proposed Platform Accountability and Transparency Act (PATA)¹ is to mandate disclosure on the part of platforms for the benefit of government-approved researchers and research projects. Under the bill, the National Science Foundation (NSF) and a new office in the Federal Trade Commission (FTC) would administer these mandates, including through the creation of privacy and cybersecurity standards for disclosure and disclosed materials.

Privacy is a complex value, though. In its control sense, it is lost when people's judgments about sharing and hiding information about themselves are defeated. I believe that an emergent property rights regime for data represents a substantial protection for privacy that people are already using in their interactions with internet platforms. By mandating disclosure from these platforms contrary to the agreements between platforms and users, the PATA legislation cuts against the grain of this kind of privacy protection. The legal immunities in the PATA legislation further erode confidence that privacy will be protected in a mandated disclosure regime.

An unconstrained disclosure mandate may be unconstitutional, and it seems unwise. The Supreme Court appears likely to revive the nondelegation doctrine soon, and an unrestricted grant of authority to mandate disclosure for the all-purpose, nebulous goal of transparency may not survive it. Constraints on the authority to mandate disclosure would be for the good. The beneficial possibilities of such mandates while our politics are generally healthy should not obscure the malign potential of mandated disclosure when our politics are less healthy.

In any event, platforms' moderation strategies and tactics should not be made transparent. Doing so

would make moderation more difficult and likely degrade the experience for platforms' users. The same logic applies to security, both the security of platforms themselves and the security that platforms seek for their users. Mandatory disclosure of security information could threaten platforms and their users.

Mandating general transparency has little precedent in our law that I am aware of. Businesses in all but a few exceptional lines have constitutional rights against being inspected or searched without warning or reason. When the business is communications, the First Amendment makes the idea of a general warrant to mandate disclosure all the more alien.

The better approach to platform transparency is to pressure platforms in ways other than through government coercion. They should participate with researchers in discovering their own consequences for society. They should seek to correct and improve where they can. To reduce the constraints that could prevent platforms from participating in research, amendments to the Computer Fraud and Abuse Act (CFAA) may be warranted to protect researchers from distended legal threats against their efforts to examine the functioning of platforms. The United States should avoid highly restrictive European-style privacy regulation in favor of our harm-based approach.

A substantial section below endorses the premise stated first above that transparency is good, but I begin with privacy and the privacy costs of a mandated disclosure.

Privacy and Related Values

An important cost of mandated disclosure would be to the privacy of platforms' users. Privacy is a complex value or set of values, so I will delve into it at some length, articulating how privacy is threatened and arguably violated even when mandated disclosure is joined with protections like those seen in the PATA legislation.

One hears appeals to privacy in many different policy and social contexts. My assessment is that people use the word "privacy" for eight distinct values.² Those values, in brief, are:

- **Control of Others' Access to Personal Information.** For countless reasons, including having a sense of control, people prefer to keep some information about themselves from others.
- **Fairness.** Each individual should get their due, whether their due is opportunity and promotion or punishment and loss.
- **Personal Security.** Denying others information about oneself can protect against physical threats and violence.

- **Financial Security.** Withholding information can be a preventive of financial frauds such as identity theft, in which someone impersonates someone else, creating accounts and debts in the victim's name.
- **Peace and Quiet.** People want to enjoy a sense of retreat from the world.
- **Autonomy.** The availability of information about people is an essential tool of legal and social pressure that may restrict people's freedom to act.
- **Integrity Against Commodification (or Anti-Commercialism).** Many people resist what seems to be the commercialization of everything and their own commercial objectification, preferring to be treated as whole individuals.
- **Reputation.** People worry that negative information about them will create negative impressions and adverse social and economic treatment.

In survey research I recently published,³ I found that financial security (i.e., prevention of identity fraud) is foremost in people's minds when asked an open-ended question about privacy concerns. When prompted to address the eight values listed above, financial security remains a top priority, joined by personal security, reputation, and autonomy. Lower-tier values, in descending order, are control, fairness, peace and quiet, and anti-commercialism. This is disappointing in a sense. Many of the lower-tier values are upper-tier for people like me. For me, the picture this research paints is of Americans as busy, practical people, who want what they want. They don't want to be scammed or injured, but they don't care that much about getting the kid-glove treatment in the information economy that we elites would like them to have.

I will focus here on what I believe to be the strongest sense of the word "privacy": control of information about oneself. A legalistic definition of privacy in the control sense that I worked up some years ago has held up fairly well. Privacy is "the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values."⁴ We all hide and share information about ourselves to portray ourselves as we wish to be perceived by others. Most people do so inarticulately, following social customs and the occasional lessons of trial and error.

Importantly, privacy is subjective. Each person chooses what to share and what not to share (again, inarticulately) based on their own interests, values, customs, and so on. Overriding their choices deprives them of control and thus privacy.

An illustration: We all retreat into our homes to gain privacy (in the control sense, as well as the “peace and quiet” sense). If a government agency—say, local police or fire—installed camera systems in each home to improve emergency detection and response, this alone would violate privacy, even before any improper use of the system. Policies designed to prevent error and abuse could reduce various risks, but it would not alter the fundamental divestment of control from the residents of the home to another decision maker. Such monitoring could only be installed consistent with privacy if the people using the four walls of the home to protect their privacy assented to this modification of their information environment.

I use an example from the physical environment because it is familiar. We all find it easier to protect privacy in physical environments because they have been around for a long time. We understand how light and sound work, and customs are stable. It is relatively hard to protect privacy online because the environment is new and still rapidly changing. The technology is complicated, and there is not a stable set of customs people can draw on to protect their privacy. But there are protections for online privacy that I think are important to recognize.

Privacy Protection Through Contract and Property

I have argued for some time in various writings⁵ and in legal briefs to the Supreme Court⁶ that there is more privacy protection online and in the communications world than many people recognize. In my view, privacy policies and terms of services statements are contracts that not only commit service providers to baseline privacy-protective behaviors; they also divide up ownership of data.

Data—this stuff that people and companies trade, own, subdivide, and profit from—is an emergent form of property. Recognizing data as property will strengthen people’s privacy protections because their loss will be more clear and they will have more remedies when, too often, some form of breach, unconsented sharing, loss, or harm occurs. If I am right that data is an emergent form of property, taking it by fiat implicates the same legal challenges as taking tangible items or land.

In the mid-to-late 1990s and early 2000s, as the internet was only beginning to become the commercial and social juggernaut that it is, foresighted legal scholars focused on the impending problem of privacy protection.⁷ They recognized the internet as a giant, pervasive information-collection machine, and many believed it threatened doom for people’s control of information about themselves.

Legal scholars with a taste for economics suggested protecting privacy by “propertizing” personal information. Giving consumers property rights in information about themselves would strengthen their

hands in the battle to protect their privacy. Others lamented that idea for a variety of reasons, including that it would “normalize” trade in data and undermine privacy (elite defined) yet further. Today scholarly consensus may be that property rights in personal information remains an interesting idea with plenty of complexity and as many drawbacks as benefits for privacy protection.

I think about these things a little differently. I believe that personal information has already acquired the characteristics of property and should be recognized as such. Companies and consumers routinely hoard or withhold personal information, process it, trade it, and enjoy other rights to personal information that are in the “bundle of sticks” that make up property rights.⁸

An empirical study has shown that courts increasingly recognize privacy notices as contracts.⁹ And the Supreme Court has treated information as property. In a 1987 case called *Carpenter v. United States*,¹⁰ the Court found that a scheme to trade on information awaiting publication in the *Wall Street Journal*’s “Heard on the Street” column deprived the *Journal* of “money or property” for purposes of federal mail and wire fraud statutes. “The *Journal* had a property right in keeping confidential and making exclusive use, prior to publication, of the schedule and contents of the ‘Heard’ column,” Justice Byron White wrote for a unanimous Court.¹¹ That was so because, even though there was no prepublication release of the information, the fraud deprived the *Journal* of its exclusive control and disposition of the information—the rights to exclude others from, and to use, the information. This protection for a corporate entity’s information should apply equally to ordinary people’s information, in my opinion.

In a more recent and—to privacy people—more familiar *Carpenter* case, Justice Neil Gorsuch argued for treatment of personal information held by telecommunications companies in property terms.

Ever hand a private document to a friend to be returned? Toss your keys to a valet at a restaurant? Ask your neighbor to look after your dog while you travel? You would not expect the friend to share the document with others; the valet to lend your car to his buddy; or the neighbor to put Fido up for adoption. Entrusting your stuff to others is a bailment. A bailment is the “delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose.” A bailee normally owes a legal duty to keep the item safe, according to the terms of the parties’ contract if they have one, and according to the “implication[s] from their conduct” if they don’t. A bailee who uses the item in a different way than he’s supposed to, or against the bailor’s instructions, is liable for conversion.¹²

In another Fourth Amendment case called *Riley v. California*, the Court wrote of a phone’s contents as “a person’s private effects.”¹³ The Court spoke of digital materials as owned items consistent with the

possessive pronoun “their” in the Fourth Amendment. We do not have to create a property regime for personal information. We just have to look around.¹⁴

Consider how privacy policies and terms of service statements allocate rights in digital data between service providers and customers. The heart of the typical privacy policy says something like: “Verizon does not sell, license, or share information that individually identifies our customers, people using our networks, or website visitors.” There is typically a short list of exceptions allowing sharing for such things as protecting the service provider, counteracting fraud, responding to valid legal process, and so on. These are the metes and bounds, covenants and easements of digital property, if you will.

When technology users leave data in the possession of service providers, all is not lost for them. According to their contracts, the general right to exclude remains theirs, an essential privacy protection.

Like spectrum, information is highly divisible, and it has different characteristics from movable and real property. (In their time, movables had to earn full-fledged status as property.¹⁵) As noted above, property rights include the right to possession, the right to use, to profit, to sell, and especially to exclude others. People and businesses exercise all these rights over data all the time.

There are several advantages to recognizing data as property allocated in part to consumers when they interact with service providers. Those advantages range from principled to practical, concrete to speculative. A principled argument is that it is consistent with Anglo-American common-law rule development to do so. Whatever scholars think or say, real people and companies talk about personal information as property. Across the internet, terms of service and privacy policies use possessive pronouns—“your information”—to describe this thing. What the contracts say is the best evidence available of what people think. And it is in the spirit of the common law to recognize this broad and deep cultural belief, incorporating it formally, if carefully and selectively, into the law.

The practical arguments are naturally more accessible. Treating personal information as property expands the range of remedies and protections that are available to consumers in a variety of situations, such as bankruptcy and contract breach. Most importantly to me, recognition of property rights in data would cause the standard privacy policy to establish that personal information in the hands of online service providers is the user-consumer’s. This data is part of people’s modern “papers and effects” for purposes of Fourth Amendment administration. Data about us in the hands of third parties is not so much soup to be ladled out by governments as soup from a tureen.¹⁶

Mandated Disclosure Undercuts Privacy

The move to mandate disclosure of personal information in the PATA legislation cuts deeply against the grain of this trend. It would signal that the US Congress sees personal information held by platforms, under contracts restricting others' access, as just so much soup awaiting the ladle.

This is true even when, as in PATA, the information will be subject to a regime of privacy and security protections. Like the placement of cameras in a home, taking data from where a consumer has deposited it and placing it in a different system divests the consumer of control. We do not have to love platforms' records on privacy to recognize that consumers have made choices and to respect their choices.

I recommend against mandating disclosure of information held by platforms despite the gains on offer for platform transparency. Doing so would undercut privacy and emerging property rights that are very important consumer protections.

Generous Immunities Undercut Privacy Protection, Too

Reading the PATA bill for the first time around Easter, I was impressed by how it distributes legal immunities like Easter eggs. Insulating particular groups from general law can be justified by a compelling interest, but it comes at a cost, and doing so is rightly controversial.¹⁷ I believe immunities should be used more sparingly, if at all, in the legislation.

Section 6(d) of the PATA bill immunizes platforms that comply with the privacy and cybersecurity regulations from suits grounded in their disclosure of the mandated information. Researchers get their immunity in section 7(d), also contingent on compliance with the privacy and cybersecurity regulations. These immunities create a simple but concerning dynamic: If the FTC regulations meant to protect disclosed information do not protect privacy and security in some respect, and if harm comes to consumers whose data has been shared under PATA, those consumers will flatly be denied recourse. The distribution of immunities in the bill says that it is more important to subject people to interesting research than it is to accord them justice when they are wronged.

In section 11, civil and criminal immunity extends to people gathering "covered information" (a defined term) if they are engaged in news-gathering or research projects "to inform the general public about matters of public concern."¹⁸ This would draw courts into assorting liability based on what constitutes "public concern," which is a social judgment courts are not well positioned to make. Indeed, it is essentially content-based assignment of immunity, which should fall afoul of the First Amendment.

Researchers without an approved focus could be sued. Researchers who meet with government approval could not.

My guess and sense as a nonexpert in this particular area is that the section 11's immunity aims to shield good-faith researchers from the CFAA. That law appears to suffer from unclear definitions, to wrongly treat civil wrongs as criminal, and to impose heavy-handed criminal penalties. If that is the purpose of this immunity, I recommend fixing the CFAA directly. Doing so would be much better than creating a complex carve-out from a complex legislative rule.

The PATA bill doesn't stop at allocating immunities. It also withdraws a sort of immunity from misbehaving platforms. Section 10 of the bill denies the protections of the Communications Decency Act's section 230 (CDA 230) from platforms that do not share information as required by the FTC under PATA. (It is narrow: The failure to comply with PATA would have to be a "significant contributor" to the claim against which CDA 230 no longer immunizes.) All this invites a brief discussion of how the CDA 230 "situation" might have been handled better.

Having worked around Congress for 25 years (and meaning no offense), I think it is better to arrive at just rules through long, society-wide deliberation than through legislative debate.¹⁹ CDA 230 illustrates why.

In the mid-1990s courts were considering whether interactive online services would be considered publishers of the information people uploaded and posted to them. If they were publishers, website operators might be liable for defamation and other causes of action because of the material users contributed to them. Had this rule taken hold, operators of online services would probably have allowed only tightly controlled and monitored interactions among users. The rollicking, interactive internet we know today would have been sharply curtailed.

In response to this concern, Congress passed legislation saying that interactive computer services are not publishers or speakers of any information others provide using their services. Thus CDA 230 became one of the most important protections for online speech in the United States.

Though it is technically a substantive definition, CDA 230 acts as an "immunity" Congress gave to online service providers. The perception of CDA 230 as a special-interest favor means that other interests are on relatively strong footing when they come to Congress seeking to overturn it. Today, CDA 230 is under attack from groups who would like to see it weakened or reversed, perhaps including one or more members of this panel.

I believe the rule against liability for online service providers is the correct one. It would be stronger if courts had arrived at a rule of “no liability” based in considerations of natural justice.

When the rules that organize our society are temporal products of legislation, they may always be “in play” for a legislative reversal. Because of CDA 230, online service providers must always remain vigilant in Washington, DC, for attempts to undercut their special “immunity.” The rules that govern online liability were established quickly, which is good, but they are obviously not settled, and there is one more reason for private businesses to maintain a stable of lobbyists and lawyers in Washington.

There is no guarantee, of course, that the common-law rule would be the same right now as what CDA 230 produced. The common-law process might still be searching for the right rule. I suspect that the platforms would not have quite the “blanket” protection that CDA 230 offers. There would be finer lines determining whether and when they are liable for the content they host. But my main point is that immunities have the effect of trampling through issues that we have a good system for analyzing: our common-law courts. They are an important part of the Anglo-American legal tradition, which is unwisely dismissed.

My strength and focus, as noted earlier, is privacy. I’m evidently willing to share opinions about other matters based on familiarity or even mere awareness. I have reservations about advancing transparency through mandated disclosure. I don’t think the trade-off between privacy and transparency on offer in PATA is a good one. But I am cognizant of the value of transparency. I have worked to create transparency in one of our nation’s largest institutions. And I know some of the difficulties involved in producing it.

We’re All in Favor of Transparency

It is easy to favor transparency in our institutions. But it is a somewhat slippery concept. It may be widely popular simply because anyone can see it is a means to their own ends. But there can be too much of a good thing. The boundless transparency sought by the PATA bill may be ill-advised and prospectively unconstitutional. Below I recommend withdrawing data pertaining to platforms’ moderation and security protection from mandatory disclosure.

Three years before ascending to the Supreme Court, Louis Brandeis wrote, “Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.”²⁰ He was arguing in *Harper’s Weekly* (December 20, 1913) for measures that would weaken the power of investment bankers. His focus on

publicity (in a sense equivalent to “transparency” today) may have been a counterpoint to his earlier *Harvard Law Review* article²¹ written with Samuel Warren entitled “The Right to Privacy.”²²

One can see broad parallels between the Progressive Era’s concern with financial and industrial trusts and modern concerns with “Big Tech.” Your evident concern with social media’s pathologies line up, semantically at least, with Brandeis’s “social and industrial diseases.”

But the sunlight metaphor has an older pedigree. Professor Alasdair Roberts of the University of Massachusetts Amherst believes that Brandeis picked it up from James Bryce’s 1888 book *The American Commonwealth*.²³ “Public opinion is a sort of atmosphere, fresh, keen, and full of sunlight, like that of the American cities,” Bryce wrote, “and this sunlight kills many of those noxious germs which are hatched where politicians congregate.”²⁴

Brandeis saw transparency as a corrective for corporate and financial wrongdoing. Bryce saw transparency as a corrective for political wrongdoing.

Their differing emphases illustrate both a strength and a weakness of transparency as a policy objective. The strength is that transparency is easy to support. It is an empty vessel into which anyone can pour their priorities, just as Brandeis and Bryce did. Conservatives and liberals may agree on platform transparency because they each foresee the other’s ox being gored in new light.

The weakness of transparency is the other side of the same coin. Favoring transparency is a commitment to no particular end. The devil in the details is the end (or ends) to which transparency may be put.

For a time, my work focused on transparency to a degree that I might have been characterized as a transparency activist.²⁵ President Barack Obama’s election in 2008 began a period of focus on government transparency. His campaign promises related to transparency of governmental operations and decision-making were exciting and encouraging. I sought to contribute to the nonpartisan and pan-ideological effort in the nonprofit sector to advance US government transparency.

Having started down the path to digital transparency some years before with a (now-defunct) website called WashingtonWatch.com, a decade ago I created and ran a project at the Cato Institute called “Deepbills.”²⁶ The project sought to enrich the publication of congressional legislation in Extensible Markup Language, or XML. XML is an encoding technique that can make the meaning of content such as bill texts automatically legible via computer.

Because of that project, for a brief period in 2014 one could look online to find the bills in Congress that

authorized appropriations or appropriated funds. You could see what members of Congress proposed to spend, and you could sort spending bills by dollar value, by date of last activity, and by the author's state.²⁷ Encoding bills in this way could only be partially automated, and the process of hand coding thousands of your lengthy bills was prohibitive, so the project ended years ago without leaving much of a mark. (The effort that did make a mark—and continues to do so—is Josh Tauberer's GovTrack.us.²⁸)

An uncomfortable parallel preceded the failure of my transparency project: The first broken promise of the Obama presidency was about transparency. In campaign speeches and on his campaign website, President Obama had pledged to put the bills Congress passed online for five days before signing them. This would give Americans a chance to find out what was in them before they became law, an arguable check against unwanted material being “snuck” into large bills. But President Obama signed his first law, the Lilly Ledbetter Fair Pay Act, just one day after Congress presented it to him.²⁹ The White House website asked the public for online comments two days after the bill became law.³⁰ As a set of institutional behaviors and public expectations, transparency is hard to manufacture.³¹

The audacious “whole of government” to “whole of the public” transparency we tried to create was “pro-democracy” and agnostic as to outcome. My view was that it might decrease demand for government. Others believed, I'm sure, that it would validate and perhaps grow existing programs and spending. It is no wonder that I focused on government spending data while others focus on campaign spending data. We were each seeing in transparency different ends that depended on our ideological starting points.

So transparency is essentially question-begging. As the subject matter of institutional transparency becomes more focused, harder questions arise. I will explore the decisions you *haven't* made in PATA's press for platform transparency through a brief diversion into constitutional nondelegation principles.

Uncircumscribed Authority to Promote Research Is Unwise

The strength of transparency as an all-purpose good thing may be a constitutional weakness. PATA creates an executive branch office and legal authorities to promote platform transparency by mandating disclosure of data to researchers. Without clear direction about precisely what should be subjected to research, PATA may fall afoul of the requirement that Congress must set policy priorities and not leave it to executive branch agencies or others.

Sections 4(d)(1) and (2) of the bill require the NSF to produce a list of “its criteria” for qualified research projects and qualified data and information. I perceive no subject-matter limit on the power the

legislation would give the NSF to authorize research projects that use platforms' data, which section 6(a) requires them to turn over.

There are many legitimate concerns with social media platforms. The press statement issued when the PATA legislation was announced makes reference, variously, to "tradeoffs," sex trafficking, information about COVID-19's origins, harm to "our families, our communities, and our democracy," and threats to "our democracy and the information ecosystem."³² The legislation does not restrict NSF-sponsored research to these topics.

As time and presidential administrations unfold, areas for research could include literally anything under the sun: immigrants' use of their native languages on social media, small businesses' customer cultivation practices, churchgoers' illicit online relationships, LGBTQ+ political organizing, drug culture and consumption in ethnic and racial communities, gun aficionados' social ties, how heterodox ideas propagate online, and more. Not all this research may be tuned to fostering the well-being of the communities under examination. The point here is that an open-ended research agenda is open-ended. If some of the research topics I have listed alarm or offend you, note that PATA excludes none of them.

Section 12, giving the FTC authority to require reports and disclosures from platforms, is similarly open-ended. Subject to privacy limitations, whatever "will assist the public, journalists, researchers, the Commission, or other government agencies" to "assess the impact of platforms" on "consumers, institutions, and society" is fair game for required disclosure. This pro-transparency policy is boundless.

"Nondelegation" is the idea that the Constitution, having granted Congress the authority to legislate and set federal policy, bars Congress from sub-granting that authority to another body, whether within the government or without. The doctrine has largely been moribund since the New Deal. But three years ago, the Supreme Court decided a case called *Gundy v. United States*.³³ The case itself did not revive the nondelegation doctrine but signaled that the Court will do so soon.

Dealing with the interpretation of a sex-offender registration statute that arguably gave the US attorney general too much policymaking authority, the case was a 4–4 decision on an eight-member Court. Justice Samuel Alito, providing the fourth vote to uphold the statute against a nondelegation challenge, said he was unwilling to revive the nondelegation doctrine without a full complement of justices, but he would join a full-Court majority willing to revive it. Since then, the membership of the Court has returned to nine, and the makeup of the Court has shifted so that there is likely a nondelegation majority for Alito to join.

The contours the doctrine will have when it is renewed are not entirely certain. Justice Elena Kagan, writing for the plurality (i.e., upholding the law), wrote:

[T]his Court has held that a delegation is constitutional so long as Congress has set out an “intelligible principle” to guide the delegatee’s exercise of authority. Or in a related formulation, the Court has stated that a delegation is permissible if Congress has made clear to the delegatee “the general policy” he must pursue and the “boundaries of [his] authority.”³⁴

A policy of unconstrained disclosure mandates, as I’ve tried to articulate above, probably falls afoul of either of these formulations.

Justice Gorsuch, who disagrees with the “intelligible principles” ‘test,’ articulated in his dissent several reasons why it is a *good practice* for Congress to retain its legislative power instead of giving it to executive branch agencies. Among others:

Without the involvement of representatives from across the country or the demands of bicameralism and presentment, legislation would risk becoming nothing more than the will of the current President. And if laws could be simply declared by a single person, they would not be few in number, the product of widespread social consensus, likely to protect minority interests, or apt to provide stability and fair notice.³⁵

I think each of us, no matter our ideology or political preferences, can think of a president serving in our lifetimes to whom we would not want to give broad power to force disclosure from platforms. We would not want his administration’s allies investigating given segments of the society and their behaviors. Legislation that provides unlimited support for transparency in the form of an unconstrained platform disclosure mandate seems to be an unwise idea, which may soon fall afoul of constitutional limits.

Should my concerns about overbreadth be at all persuasive, there are aspects of platform transparency that I recommend explicitly restricting as a start. Making platform moderation strategies transparent threatens to undercut those strategies. Transparency should not make the social media experience harder to oversee for the companies and worse for consumers. The same logic applies to security.

Do Not Mandate Disclosure of Moderation Strategies or Tactics

One of the leading thought pieces on how social media could be done better is “Protocols, Not Platforms: A Technological Approach to Free Speech,”³⁶ an August 2019 piece by Mike Masnick, editor of the prolific, long-running TechDirt blog. His brief is that we have seen a shift from widespread use of

common protocols, such as the email protocol (i.e., SMTP), to platforms such as Facebook and Twitter. This is partly because platforms can curate the user experience better than users grappling with technical protocols themselves. Given revenue sources such as advertising, platforms have an incentive to maintain themselves in the way protocols do not.

Masnick argues for a shift back to protocols, dangling the possibility that integrating cryptocurrencies into protocols might create revenue sources that support maintenance of protocols as such. This could supplant the need for targeted advertising, with its privacy costs for people concerned about commodification. More importantly for our purposes here, it could move editorial decisions, including moderation decisions, back to the edge of the network—back to users themselves.

A shift so grand does not have to happen for things to be different. I have watched, bemused, as consensus has emerged among pretty much all elite segments (policymakers, journalists, platform leaders, and so on) that the platforms must moderate content for their users rather than giving users tools to moderate content themselves. (CDA 230 may have had some part in this.)

I noted above my government transparency website, WashingtonWatch.com. It enjoyed brief periods of attention. One bill to extend unemployment benefits, for example, received more than 200,000 comments from users who grouped themselves into warring factions. (That's, maybe, three minutes' worth of material on a major platform nowadays.) Supporters and opponents of the Ethiopian government clashed on my site. Some alleged to me that users of my site had dishonestly adopted their identities to misrepresent their positions on Ethiopian politics.

Committed to free speech, leery of personally moderating all that content, and having zero budget for staff, I built rudimentary tools for self-moderation. WashingtonWatch.com allowed people to block the words of their choosing, other speakers, and so on. I did intervene when pure scatological content was posted, when a clear violation of someone's legal rights occurred, and in one instance when someone posted a federal elected official's private cell phone number. (I could not adjudicate claims of Ethiopian identity fraud.)

This hardly makes me an expert in platform moderation, and the problems I encountered were modest compared to what the large platforms see. What I observed, though, was that some users were relentless in their efforts to reverse engineer and then evade every moderation policy and practice. Given automated word-based moderation, they would vary words and spellings. They recognized the hours of the day that I was active, and they posted obnoxious content when I was "off the clock."

It was fascinating to see the herculean effort that went into defeating a small website's attempt to create a functional, debate-oriented community. I was not the most sophisticated webmaster, and I do not know whether I was confronted by a few extremely dedicated individuals or groups of collaborators. Whatever the case, I recognize from my experience that content moderation is extremely difficult, a fraught, spy vs. spy-type challenge. Broad strategies and narrow tactics are probed and tested relentlessly by those trying to turn social media platforms to their own advantage—or just trying to ruin them.

The concept of the “attack surface” in computer security is a helpful metaphor. A simple computing system that integrates with few other systems has a small attack surface because it has fewer vulnerabilities. A complex, highly interactive system will have exposure to many more vulnerabilities and thus a larger attack surface.

Think of platforms' moderation systems as having an attack surface to protect. It is easy to see how forced disclosure of data about those systems would increase the attack surface. Once a university-affiliated researcher has a line into data related to a platform's moderation system, the attack surface is not just the platform's systems. It now includes the communications links to the researcher, the university's computing infrastructure, the researcher's personal computing and communications tools, and any student-assistants' computers and communications. The PATA bill addresses this risk to a degree by requiring the creation of security protocols, but the creation of risk here is ineluctable. One can predict that those security and privacy protocols will fail at times, with greater or lesser consequences.

The better way to secure systems is to leave their attack surfaces smaller. I recommend excluding moderation systems in statutory language from the forced transparency regime.

I make the same recommendation as to platform security, both measures taken to secure the platforms themselves and the measures platforms take to provide security to users. Statutory language should specify that no data from or about security systems should be subject to mandated disclosure. The risks disclosure would create seem more likely and greater than the diffuse, contingent benefits of a disclosure mandate.

We are still in a time when responsibility for data breaches and security failures is hard to pin down. If disclosure is mandated around platform security, that will create a diffusion of responsibility. When breaches and losses occur, the platforms, researchers, and universities involved may all point fingers at each other. My preference would be for the one responsible party, the platform, to be on the hook for

whatever wrongs and harms occur.

Here I have suggested carving out information and data related to moderation and security from any disclosure mandate. The same principle applies with respect to the personal and private information of users, which I treated at length above, focusing on the property rights that should protect them. I do not see the privacy-versus-transparency trade-off offered by PATA as a good one.

At some risk of “constitutionalizing” every issue, I will now turn to the First Amendment values that are threatened by mandated platform transparency, even if you accept my advice to exclude moderation data, security data, and personal data from your transparency ambit.

Mandating Platform Transparency Impinges on Free Speech

In case it needs saying, the object of your transparency efforts are platforms for speech and communication. Below, I will briefly articulate how I see speech as a direct object of the mandated disclosure in the PATA bill. Perhaps lacking in breadth of vision, I see general transparency mandates placed on in any industry as anomalous. It would be even more strange and difficult to mandate transparency on constitutionally protected speakers. I begin with a brief exploration of our interest in “algorithms.”

When your computer pings a server asking for a given web page, an algorithm determines exactly what content the server returns based on things like the type of browser you are using and the screen resolution of your device. When you search on Google Maps for a store, an algorithm might include in your result that the store is open or closed based on its hours and the current time of day. That algorithm is a little more interesting, but it is nothing like the algorithms that the PATA bill seeks in the name of platform transparency.

The bill is (ahem) transparent about what algorithms are interesting. Section 12(g)(1) defines “algorithm” as a computational process with a “purpose of determining the order or manner that a set of information is provided, recommended to, or withheld from a user of a platform, including the provision of commercial content, the display of social media posts, recommendations of user or group accounts to follow or associate with, or any other method of automated decision making, content selection, or content amplification.” I would summarize that definition as “automated editorial choices.” Section 12 authorizes the FTC to require platforms to disclose their automated editorial choices.

I will draw again on my Fourth Amendment knowledge to reach what is really a First Amendment point. There are a small number of industries so closely regulated that they are treated as not having a Fourth

Amendment right against inspections without a warrant. These are liquor sales,³⁷ firearms dealing,³⁸ mining,³⁹ and running an automobile junkyard.⁴⁰ Each either has a present or historical association with crime, or physical danger is a manifest element of its operations.⁴¹

In *City of Los Angeles v. Patel*,⁴² the Supreme Court invalidated a statute requiring hotel operators to make their registries available to the police on demand. The Court brushed aside the argument that hotels are so closely regulated that they lack the rights that apply generally to individuals and businesses. The requirement struck down in *Patel* is the closest analogy I can think of to the general warrant requirement that PATA authorizes. Section 12 gives the FTC power to require that platforms should report to the government in detail on their editorial choices.

A general order to disclose business practices and records would fall afoul of the law for all but the small group of exceptional business lines noted above. But platforms are businesses whose stock in trade is speech. The Internet and social media are strange but real descendants of the printing press, disembodied and given to everyone to use as much as they want. Social media companies aggregate and augment this mass exercise of expression. Given the communicative dimension of these services and the First Amendment's brusque tone in saying "Congress shall make no law ... abridging the freedom of speech, or of the press....", I do not believe platforms fit in the category of "closely regulated" industries "long subject to close supervision and inspection"⁴³ that can be divested of their rights for purposes like crime control and worker safety.

There is an argument that platforms are so important and dangerous that they should be treated the way traditional fonts of crime and danger are. That argument could be availing if there were a tight means-ends nexus between accessing platform data and fixing the pathologies for which they are blamed. Close monitoring of auto dismantlers makes it much harder for them to operate as fencing operations. But platform transparency offers little in the way of concrete benefits or protections. It would be nice, but I do not think honest social scientists can promise concrete results of the type that justify government-mandated disclosure in the areas where it exists.

For me, it is even hard to lay Brandeis's "social and industrial diseases" at the feet of platforms. Their nature as communications platforms intervenes. Any harm or pathology that social media arguably produce or contribute to has a responsible actor: the social media user. A point I often make casually is that social media holds a mirror up to society, and people don't like what they see. One may blame the mirror, but more productive change may come from examining more deeply the roots of the many problems that social media seem to expose.

That may seem like a cold approach, inured against risks to democracy or the struggles that young people face online. But the urgency that sincere researchers feel about these problems does not imply their capacity to devise solutions. It may be that the personal, family, and community responsibility is what gets us through these challenges. I welcome orthodox university research as one part of finding solutions, but it is as likely that we collectively absorb what the new media environment means and develop strategies en masse for getting what is good from social media while mitigating their ill effects.

I do not share the premise that private, competitive communications platforms are a public resource through which researchers and government can tune society. That notion is at odds with our traditions, better judgment, and probably also the First Amendment. In these “hard” social times, I believe resorting to first principles will still serve us.

Transparency Done the Right Way

The demerits I see in mandated disclosure do not undercut the need for, or the value of, research into the new social media environment and its effects on all our health, interests, and values. We should have such research. So how do we get there?

Most of my experience with working to generate transparency is in the government sector. In a democracy the public’s entitlement to transparency is something of a given. The private sector is different.

In case it needs arguing, social media platforms are on the private side of the private/government line. Yes, they exercise substantial dominion over the digital “spaces” they control, but the spaces they control are metaphorical. One exits these spaces by clicking on a link, turning one’s eyes away from one’s phone, or doffing the virtual-reality headset. If one must forgo interacting with one’s peers to do so, that seems to be as much an exercise of communities’ collective power (and inertia) than any platform’s power to keep them there.

Governments control physical spaces, which are much harder to leave, practically and sometimes legally. Good governments assert a monopoly on the use of force within their jurisdictions to provide inhabitants of those jurisdictions security against wrongdoers and invaders. No platform ever detains, arrests, or jails a user. No platform ever goes to war against another platform. These are distinct entity-types: platforms are not governments. Platforms exercise some of the same authority over their “spaces” (again in scare quotes because they’re metaphorical) as I do over my home. You have to follow certain rules while you’re there, and you can easily leave.

Broadly, I see transparency in the private sector as any other good. It is a product of market demand.

As a thought experiment, ask yourself why we do not have to ask merchants to be transparent about the prices they charge. That information is “of the essence” for almost any consumer transaction. Failing to be transparent about pricing will generally produce an avalanche of shunning that puts tight-lipped sellers out of business.

Most other dimensions of consumer interest seem to work the same way, if with less unanimity. There may be a literature that analyzes how businesses work to satisfy the information demands consumers place on them, but as a casual observer I can see businesses respond to many dimensions of consumer interest: recycled materials/recyclability, country of origin, organic content, low cost, ease of use, good treatment of workers, and so on. I see no reason why consumer demand cannot press platforms likewise to be good stewards of their communities in any sense that matters.

Consumer demand does not need to be entirely spontaneous. As sophisticated actors in Washington, D.C., we all know that interest-based organizations of every stripe press for broader public recognition of the things they think are important. From direct appeals to consumers, to planting news stories, to placing op-eds and magazine articles, advocates shape the society directly. Nothing excludes researchers and universities from participating in these processes. There’s a healthy community of academics who place articles in the popular press alerting the public to the dangers of social media, which naturally presses platforms to improve.

The media tends to portray tech titans as omniscient. If they are, their failings to protect consumers can only be the product of mendacity and evil arrogance. I suspect that the truth is a little less attractive and less black-and-white. Some of our social media and technology leaders are probably in way over their heads, overwhelmed by the enormity of what they have created and racing just to keep up. If they were in control, they would almost certainly ally with researchers to understand better the social and political consequences of their platforms. This is not to deny the profit motive, but the ESG movement (economic, social, governance) shows that corporations of all stripes can be brought to heel and pressed to do good while they do well, if that’s what their customers want from them.

It may be obvious that the dynamics of social change in private markets is an interest of mine, but not my expertise. My ignorance particularly extends to the question whether the community of researchers wanting access to platform data has exhausted the approach of seeking partnership with platforms. The record that supports mandated disclosure would be incomplete if it is not shown that voluntary collaboration sought for a lengthy period has entirely failed. From what I know, mandated disclosure is a

cudgel that has not yet been justified by years-long, knowing intransigence on the part of platform leaders.

Moving back toward my potential strengths, I will offer a couple of policy prescriptions that I believe can support the market-driven research environment that I would prefer. As noted earlier, I might recommend modifying the CFAA to ensure that it addresses only true criminal behavior and does so proportionately. My sense as a non-expert is that it may criminalize behaviors that are properly treated as civil wrongs, and it may treat as wrongs things that are not wrong. If it indeed has draconian penalties, they should be reined in.

Privacy laws like those seen in Europe and California may be a substantial impediment to platforms' collaboration with researchers. The General Data Protection Regulation in Europe and the California Consumer Privacy Act are characterized by heavy prescription about what platforms (and others) can and cannot do with data. Our common-law system, by contrast, is generally harm-based. It does not list what can and cannot be done. It allows anything to be done provided that someone who harms another must make them whole. Under a harm-based system like ours, platforms have much more room to ally with university researchers and others to jointly explore the manifold effects of social media on society.

One option that seems almost radical is to ask consumers themselves if they want to participate in research. The question of platform transparency has a characteristic that you see in privacy debates sometimes, too. Government entities, advocates, and big companies debate about these consumer interests, treating actual consumers as an afterthought. If data about users is their property because of contractual commitments, as I believe, it should be harder to leave them out of the conversation. If social media users are to be the subject of research, perhaps they could be asked by a willing platform if they want to participate.

Notes

¹ Platform Accountability and Transparency Act, 117th Congress, 1st sess. (2021), https://www.coons.senate.gov/imo/media/doc/text_pata_117.pdf.

² See Jim Harper, *Privacy and the Four Categories of Information Technology*, American Enterprise Institute, May 26, 2020, <https://www.aei.org/research-products/report/privacy-and-the-four-categories-of-information-technology/>.

³ See Jim Harper, "What Do People Mean by 'Privacy,' and How Do They Prioritize Among Privacy Values? Preliminary Results," American Enterprise Institute, March 18, 2022, <https://www.aei.org/research-products/report/what-do-people-mean-by-privacy-and-how-do-they-prioritize-among-privacy-values-preliminary-results/>.

⁴ Jim Harper, "Understanding Privacy—and the Real Threats to It," Cato Institute, *Public Analysis* 520, August 4, 2004, <https://www.cato.org/policy-analysis/understanding-privacy-real-threats-it#>

⁵ See, for example, Jim Harper and Neil Chilson, *The Semantics of "Surveillance Capitalism": Much Ado About*

Something, American Enterprise Institute, December 1, 2021, <https://www.aei.org/research-products/report/the-semantics-of-surveillance-capitalism-much-ado-about-something/>; and Jim Harper, "On the Cedar Point Nursery Decision: Now Do Intangibles," American Enterprise Institute, June 30, 2021, <https://www.aei.org/technology-and-innovation/on-the-cedar-point-nursery-decision-now-do-intangibles/>.

⁶ "US Supreme Court Review of Petition for Writ of Certiorari in *Timothy Ivory Carpenter v. United States of America*," No. 16-402, August 11, 2017, https://www.cato.org/sites/cato.org/files/pubs/pdf/carpenter-v-united-states_1.pdf; and "Brief for the Cato Institute as Amicus Curiae Supporting Petitioners at *Timothy Ivory Carpenter v. United States of America*," No. 16-402, October 28, 2016, <https://www.cato.org/sites/cato.org/files/pubs/pdf/carpenter-v-united-states.pdf>.

⁷ See, for example, *Symposium: Cyberspace and Privacy: A New Legal Paradigm?*, *Stanford Law Review* 52, no. 5 (May 2000), <https://www.jstor.org/stable/1252780>.

⁸ Tony Honoré, *Making Law Bind: Essays Legal and Philosophical* (New York: Oxford University Press, 1987), 161, 162.

⁹ Oren Bar-Gill, Omri Ben-Shahar, and Florencia Marotta-Wurgler, "Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts," *University of Chicago Law Review* 84, no. 1 (Winter 2017): 7–35, <https://chicagounbound.uchicago.edu/uclrev/vol84/iss1/2/>. But see also Gregory Klass, "Empiricism and Privacy Policies in the Restatement of Consumer Contract Law," *Yale Journal on Regulation* 36, no. 1 (Winter 2019): 45–115, <https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3005&context=facpub>.

¹⁰ *Carpenter v. United States*, 484 US 19 (1987).

¹¹ *Carpenter*, 484 US at 26.

¹² *Carpenter v. United States*, 585 US (2018) at 14 (Justice Neil Gorsuch's slip opinion).

¹³ *Riley v. California*, 573 US 373 (2014) at 2473, 2492.

¹⁴ See Jim Harper, "Perspectives on Property Rights in Data," American Enterprise Institute, August 8, 2019, <https://www.aei.org/technology-and-innovation/perspectives-on-property-rights-in-data/>.

¹⁵ In medieval times, ordinary possessions were "not esteemed of so high a nature, nor paid so much regard to by the law, as things that are in their nature more permanent and *immoveable*, as land and houses, and the profits issuing thereout." Travel and commerce necessitated putting personality "in a light nearly, if not quite, equal to . . . realty." William Blackstone, *Commentaries on the Law of England in Four Books, Vol. I* (Oxford, UK: Clarendon Press, 1765). Richard Pipes states,

Sometime during the period in European history vaguely labeled 'early modern,' there occurred a major break in the attitude toward property. It was the consequence of the remarkable expansion of commerce which began in the late Middle Ages and accelerated following the discovery of the New World.

Richard Pipes, *Property and Freedom* (New York: Alfred A. Knopf, 1999), 25. Eric Jones examines theories that might explain how personal property rights took hold. Eric Jones, *The European Miracle: Environments, Economies and Geopolitics in the History of Europe and Asia*, 3rd. ed. (Cambridge, UK: Cambridge University Press, 2003).

¹⁶ Since at least 2007, I have lamented the "cloud" metaphor for online services because it distorts expectations by eliding the complex of service providers and the protective obligations they have to consumers. See Jim Harper, "Good Stuff from Google / The Internet Is Not a Cloud!," The Technology Liberation Front, August 9, 2007, <https://techliberation.com/2007/08/09/good-stuff-from-google-the-internet-is-not-a-cloud/>; Jim Harper, "I Hate 'Cloud Computing,'" The Technology Liberation Front, February 6, 2009, <https://techliberation.com/2009/02/06/i-hate-cloud-computing/>; and Jim Harper, "Dropbox: A Privacy Black Box," The Technology Liberation Front, December 12, 2009, <https://techliberation.com/2009/12/12/dropbox-a-privacy-black-box/>. Given the time frames involved, it is appropriate to admit that I have been like Abe Simpson, shaking my fist at the cloud. See Know Your Meme, "Old Man Yells at Cloud," <https://knowyourmeme.com/memes/old-man-yells-at-cloud>.

¹⁷ It is gratifying to see the judge-made doctrine of "qualified immunity" for government agents who harm citizens come under scrutiny and criticism in recent years. David Deerson, "The Cause Against Qualified Immunity," *National Review*, July 13, 2020, <https://www.nationalreview.com/bench-memos/the-case-against-qualified-immunity/>.

¹⁸ Platform Accountability and Transparency Act, 117th Congress, section 11(a)(2).

¹⁹ Jim Harper, "Remember the Common Law," Cato Institute, March/April 2016, <https://www.cato.org/policy->

[report/march/april-2016/remember-common-law#](#).

²⁰ Louis D. Brandeis, "What Publicity Can Do," *Harper's Weekly*, December 20, 1913,

https://www.sechistorical.org/collection/papers/1910/1913_12_20_What_Publicity_Ca.pdf.

²¹ Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (December 15, 1980): 193–220, <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>.

²² Sunlight Foundation, "Brandeis and the History of Transparency," May 26, 2009,

<https://sunlightfoundation.com/2009/05/26/brandeis-and-the-history-of-transparency/>.

²³ See Alisdair S. Roberts, "Where Brandeis Got 'Sunlight Is the Best Policy,'" March 1, 2015,

<https://aroberts.us/2015/03/01/where-brandeis-got-sunlight-is-the-best-disinfectant/>. Other antecedents of Louis Brandeis's notable quote can be found at Quote Investigator, "Sunlight Is the Best Disinfectant," <https://quoteinvestigator.com/2020/09/22/sunlight/>.

²⁴ James Bryce, *The American Commonwealth* (1888): 355.

²⁵ Mark Tapscott, "Watchdog: Cato Institute's Jim Harper Is on a Quest as a Digital Diogenes," *Washington Examiner*, December 19, 2012, <https://www.washingtonexaminer.com/watchdog-cato-institutes-jim-harper-is-on-a-quest-as-a-digital-diogenes>.

²⁶ See Cato Institute, "Deepbills Project," <https://www.cato.org/resources/data>; and Jim Harper, "Cato's 'Deepbills' Project Advances Government Transparency," Cato Institute, May 21, 2013, <https://www.cato.org/blog/catos-deepbills-project-advances-government-transparency>.

²⁷ See Jim Harper, "Appropriate Appropriations? Transparency and Spending Control," Cato Institute, January 23, 2014, <https://www.cato.org/blog/appropriate-appropriations-transparency-spending-control>.

²⁸ GovTrack.us, website, <https://www.govtrack.us/>. A worthy history of the effort to pull data out of the government can be found at Joshua Tauberer, "GovTrack Now Actually Uses Open Government Data," Medium, July 6, 2016, <https://medium.com/civic-tech-thoughts-from-joshdata/govtrack-now-actually-uses-open-government-data-5fc16f37e86#iflkryvgs>.

²⁹ Lily Ledbetter Fair Pay Act of 2009, Pub. L. 111-2, <https://www.congress.gov/bill/111th-congress/senate-bill/181/actions>.

³⁰ Angie Drobnic Holan, "Obama Breaks Promise on 'Sunlight Before Signing,'" Politifact, January 29, 2009, <https://www.politifact.com/article/2009/jan/29/obama-first-broken-promise/>.

³¹ In 2011, I wrote about the data publication practices that would support government transparency, using water as a metaphor. Information and data must be potable, and it must be sought out by the public. Curiously, I did not use the line, "You can lead a horse to water . . ." See Jim Harper, "Publication Practices for Transparent Government," Cato Institute, September 23, 2011, <https://www.cato.org/sites/cato.org/files/pubs/pdf/bp121.pdf>.

³² Chris Coons, "Coons, Portman, Klobuchar Announce Legislation to Ensure Transparency at Social Media Platforms," press release, December 9, 2021, <https://www.coons.senate.gov/news/press-releases/coons-portman-klobuchar-announce-legislation-to-ensure-transparency-at-social-media-platforms>.

³³ *Texas v. Commissioner of Internal Revenue*, 596 US (2022), https://www.supremecourt.gov/opinions/21pdf/21-379_c07d.pdf.

³⁴ *Texas*, 596 US.

³⁵ *Texas*, 596 US. (See Justice Gorsuch's dissenting opinion.)

³⁶ Mike Masnick, "Protocols, Not Platforms: A Technological Approach to Free Speech," Columbia University, Knight First Amendment Institute, August 21, 2019, <https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech>.

³⁷ *Colonnade Catering Corp. v. United States*, 397 U. S. 72 (1970).

³⁸ *United States v. Biswell*, 406 US 311, 311–312 (1972).

³⁹ *Donovan v. Dewey*, 452 US 594 (1981).

⁴⁰ *New York v. Burger*, 482 US 691 (1987).

⁴¹ See *New York*, 482 US at 709 ("Automobile junkyards and vehicle dismantlers provide the major market for stolen vehicles and vehicle parts"); and *Donovan*, 452 US 594, 602 (1981) (describing the mining industry as "among the most hazardous in the country").

⁴² *City of Los Angeles v. Naranjhabai Patel*, 576 US (2015), https://scholar.google.com/scholar_case?case=942161772811530919&hl=en&as_sdt=6,30

⁴³ *Colonnade Catering Corp. v. United States*, 397 US 72, 74, 77 (1970).

Before the United States Senate Committee on the Judiciary,
 Subcommittee on Subcommittee on Privacy, Technology and the Law,
 Hearing on Platform Transparency: Understanding the Impact of Social Media

May 5, 2022

Statement of Daphne Keller
 Stanford University Cyber Policy Center¹

Chairman Coons, Ranking Member Sasse, and Members of the Subcommittee:

Thank you for the opportunity to testify. I am a legal academic, and primarily write about platform regulations, including international approaches, as they affect online content and speech. I also worked on transparency reporting at Google over ten years ago, and have more recently consulted or advised smaller platforms on their reporting, so I bring practical experience on today's topic.²

It is an honor to be here. I am particularly honored to testify alongside Nate Persily and Brandon Silverman. They have both built actual, working transparency tools – tools that can and should be expanded upon. The future should include more such tools. We should deploy more of the broad array of transparency mechanisms that I'm sure will be discussed in this hearing, including scraping tools, APIs, public repositories of data and content, and direct disclosures to individual users. The EU's new Digital Services Act (DSA) has prescribed many of these things by law. The U.S. can and should follow suit, enacting our own well-drafted laws to expand public understanding of major platforms' governance of online speech.

Transparency is essential to getting every other part of platform regulation right. I am grateful to the people who have put together proposals like the draft Platform Accountability and Transparency Act (PATA), the Digital Services Oversight and Safety Act (DSOSA), the NUDGE Act, and the Kids Online Safety Act for taking the first steps. But much as I'd love to spend my testimony cheering for transparency, I think my job here today is to point out difficulties that will need to be navigated if these bills are to reach their potential. I hope the drafters will take my comments as an act of support and an effort to make things better. At the end of the day, imperfect, first generation transparency laws may be better than no transparency laws. But they are also so important, it is worth the work to get them right.

There are a few things I see as gravely concerning in various proposals – elements that really don't belong in these laws, and could make them quite damaging. One is making transparency obligations a condition for immunity under laws like the Communications Decency Act provision commonly known as CDA 230. Connecting the two risks harming ordinary people, in ways that have very little connection with the goals of transparency laws. A second is drafting transparency laws in ways that effectively reduce people's legal protections from state

¹ Affiliation for identification purposes only; appearing in personal capacity.

² Recently I have consulted for Pinterest, including on transparency-related topics.

surveillance. A third is enacting transparency rules designed for giants like Facebook or Google, but imposed on very different and smaller companies.

Platform transparency in practice is complicated and messy.³ If we ask companies for the wrong data, we won't learn useful things. It's hard to know in advance quite what the right questions are. Getting them right will be iterative, and what "right" means will almost certainly change with future technologies, business models, and human behaviors. Having an expert regulator to navigate those changes makes sense. But there are also major questions of policy that should be made by Congress. My goal here is to describe those as I see them, and to suggest some directions of travel.

Key Conclusions

High level takeaways from my testimony are as follows. Most of these are explored in more depth below.

- Transparency rules should be overseen by an expert agency with the flexibility to adapt to future changes, including technological ones. But that flexibility should be constrained by policy choices made by Congress. In some cases that may mean setting hard legislative limits, like rules limiting obligations to platforms over a certain size. In others, it may mean guiding the agency's choices by defining a list of factors it must consider, for example in weighing impact on competition against the public benefit of disclosures.
- Transparency laws should not become surveillance laws. Nothing in them should reduce Americans' legal protections under the Fourth Amendment or laws like the Stored Communications Act. Users' expectations of privacy should also shape any laws compelling platforms to report on those users' activity, including in cases where that activity was publicly visible.
- The privacy issues raised by researcher access to user data are complex and warrant both Congressional and agency attention. Laws requiring that platforms disclose user data to researchers present very serious tradeoffs between legitimate but competing goals. In many cases, there will be no way to support important research without compromising equally important protections for users. Some important underlying questions in this area would be better resolved through federal privacy legislation. Congress should engage with these difficult policy questions, consult with privacy and transparency experts, and provide guidance to implementing agencies.
- Broad public access to information is essential. Some of the most important research on platforms to date has been accomplished by researchers "scraping" publicly visible data from platforms, or using archives of material that are available to the general public. These approaches are not without privacy tradeoffs of their own. But there is inherent value in public data access, without federal agencies, companies, or universities acting as

³ A list of concrete reasons why even basic accounting questions become complex is in Daphne Keller, *Content Transparency Logistics*, Stanford CIS Blog (March 19, 2020), https://docs.google.com/document/d/1tkZB3Hh73o9OzZzf6qMI8eN_eIX8fnRkUowzKxHURdk/edit.

gatekeepers. The complexity of privacy tradeoffs, and the imperfection of many potential resolutions, should not lead us to abandon efforts to expand and improve truly public access to information.

- Laws designed for a handful of megaplatforms should not automatically or easily extend to their smaller competitors. Treating smaller platforms like incumbents has consequences for competition, innovation, Internet users' rights, and public discourse. Any transparency laws should set careful thresholds in defining which platforms have enough users, revenue, or social impact to justify particular obligations. Hard policy calls about appropriate burdens on platforms should not be left entirely to agency discretion. At minimum, Congress should instruct agencies to consider factors like what risks platforms pose, what specific disclosures and burdens are appropriate as a result, and what research goals justify disclosure mandates. Agencies should perhaps also, to put it bluntly, experiment on the giants first. After familiarizing themselves with the mechanics of data collection and the complexity of privacy tradeoffs on platforms like YouTube and Twitter, as well as consulting with civil society and experts, regulators would be better positioned to tailor any obligations for other platforms.
- Transparency mandates should not be tied to immunities under CDA 230. The practical effects of this approach would likely disserve both transparency goals and the goals of CDA 230's critics.
- Transparency mandates raise several concerns about free expression and the First Amendment. One is that poorly devised rules may lead platforms to adopt blunter content moderation standards; stay out of the content hosting and moderation business entirely; or converge on similar rules that reduce the diversity of online speech. Another is that platforms themselves may raise significant First Amendment objections. Congress should be aware of and navigate these concerns.
- Platforms should not be liable for disclosures that are compelled by law. They should not be vulnerable to suit when they had no choice about providing data. If platforms' obligations are unclear, they should be able to seek agency confirmation about what actions are compulsory, and thus immunized. This principle applies both to affirmative disclosure obligations and to other important transparency laws, such as those governing scraping.
- The law should facilitate more open, ongoing communication between researchers, platforms, and the administering agency. Defining and collecting platform data sets can be complex, frustrating, and time-consuming. It requires clear and careful communication about technical details. Laws intended to enable data access and novel inquiry by researchers will serve all participants in the process better if they support collaboration and open discussion when possible. Any more adversarial process should be a fallback mechanism.
- U.S. law should be broadly aligned with the EU's new requirements under the Digital Services Act. I will describe those requirements below. Not all of them are cultural or

constitutional matches for the U.S. But to the extent that our legal instruments can be reconciled, the result will be more useful information for the public and more consistent and streamlined obligations for platforms. It would also reduce the likelihood of future U.S./EU disputes about privacy and data protection in this area.

I. Privacy

One of the biggest policy issues for transparency laws involves user privacy. Some decisions, including about the data seen by researchers, involve complex tradeoffs. Other privacy issues should, I believe, be non-negotiable in transparency legislation. This includes preserving Internet users' existing protections from government surveillance.

A. Researchers' Access to Private Data

Some highly valuable research is difficult or impossible to carry out without researchers themselves seeing private information about Internet users. We cannot have both optimal research and optimal privacy: Lawmakers must make value judgments and tradeoffs between the two. Some of the issues involved would be better addressed by federal privacy legislation. In the meantime, transparency laws present thorny questions about what personal data researchers get to see. I explained these in detail in a recent piece, and will review them more briefly here.⁴

User privacy cannot be protected solely through after-the-fact liability for researcher misconduct, or data management requirements for things like secure storage or encryption. It also requires sensible rules about what data researchers see in the first place. While the details of such rules are best left to agencies, the policy direction should come from Congress. This could take the form of firm rules or more flexible factors to guide agency decisions.

- Private communications: To illustrate the issue, consider a project that involves content shared privately by users on a platform like Facebook. Disclosing the content of one-on-one messaging on the platform would be the modern equivalent of disclosing personal mail. Presumably Congress does not intend to depart so far from the spirit of the Fourth Amendment, or the letter of laws like the Stored Communications Act. (SCA) Should disclosure become more acceptable if a post was shared with twenty friends? With a hundred, or five thousand? Does the answer depend on the goal of the research and the sensitivity of the privately shared content?
- Sensitive content: Researchers do not need to know the identity of a user to uncover personal information when they review the content of privately shared posts. Such content may, for example, include breastfeeding images, or discussion of a named individual's personal struggles with cancer, bereavement, or difficult life choices. If researchers *can* see this content, user privacy is compromised. If they *can't* see it,

⁴ Daphne Keller, *User Privacy Versus Platform Transparency*, Stanford CIS Blog (April 6, 2022), <https://cyberlaw.stanford.edu/blog/2022/04/user-privacy-vs-platform-transparency-conflicts-are-real-and-we-need-talk-about-them-0>.

extremely important research becomes impossible. In particular, if only platforms see the content they take down, they will continue to “check their own homework” in reporting on their content moderation practices. This could preclude third party researchers on foundational questions about errors, bias, or disparate impact of content moderation.⁵

- Large data sets: Similar problems arise with large data sets that are “anonymized” or show only aggregate data about users. As any privacy practitioner knows, it can be very easy to identify individuals’ private information using such data sets. In the 1990s, for example, MIT researcher Latanya Sweeney used publicly available “anonymous” data sets to identify the health records of the governor of Massachusetts. More recently, researchers identified individuals based on their “anonymized” viewing data released by Netflix. These failings are better understood today. Technical tools like differential privacy or homomorphic encryption can help to avoid them. But those tools can also interfere with some kinds of research, including analysis of smaller or marginalized populations.

There are many other privacy questions of this sort. Should researchers have access to public posts that users have since deleted?⁶ My tentative conclusion is that users should not lose so much control over their own posts. But that would make some bad actors online much harder to detect and study. Should an individual social media user’s history of policy violations be made public?⁷ Should transparency laws require platforms to track data about users or engagement, at the same time that many public interest groups want that tracking to stop?⁸ If researchers who scrape social media content discover that a public figure used a pseudonym to discuss private topics in a public forum – like a Reddit support group for people struggling with infertility – should they be free to publish that information?⁹ None of these questions are easy.

For some, the response to many of these questions is “Platforms can see this information anyway, and they use it for research. So it might as well be used for research in the public interest, too.” Maybe that’s the right way of looking at things. On the other hand, it doesn’t track privacy laws’ usual expectation (or perhaps legal fiction) that users consent to share their data with platforms based on particular expectations about how the data will be used, who will see it, how well it will be secured against breaches, and so forth. Unless user expectations and understanding shift significantly, that framework will be hard to reconcile with laws requiring platforms to hand users’ data to third parties, for uses the person did not expect, under the

⁵ Notably, the most important empirical research on content takedown policies comes from the rare cases where such content information *is* available to researchers, because it is public and remains available online. See discussion of Lumen Database in Daphne Keller and Paddy Leerssen, *Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation*, in Nathaniel Persily and Joshua A. Tucker, eds., *Social Media and Democracy*, Cambridge U.P., 2020, <https://www.cambridge.org/core/books/social-media-and-democracy/facts-and-where-to-find-them-empirical-research-on-internet-platforms-and-content-moderation/78DE9202F2D00F2967EFC5CBDCE2CAF0>.

⁶ PATA Discussion Draft 12(b)(4) puts this decision in the FTC’s hands.

⁷ PATA Discussion Draft 12(b)(3)(F).

⁸ DSOSA; PATA Discussion Draft definitions of reach and prevalence, and non-optional tracking at 12(b)(2).

⁹ PATA Discussion Draft part 10(b)(3)(C) says FTC guidelines will tell researchers not to publish identifying information scraped from public sites without consent, except for public officials and public figures.

stewardship of less capable security teams. Mandates like this may also raise real tensions with the EU's General Data Protection Regulation (GDPR).¹⁰

Privacy challenges like these pose some questions that are technical, and appropriate for agency assessment. Recognizing when people may be reidentified using seemingly anonymous data sets, for example, is not a matter for Congress. Nor is the negotiation process that I think should precede any disclosures of private data to researchers. But other questions, involving values and public policy priorities, fit squarely in Congress's job description.

B. Government Access to Personal Data

Platform transparency laws should not create a back door for new government surveillance powers. It would be perverse if a bill intended to curb platform power instead became a means for state actors to harness that power, effectively using private platforms to collect information about citizens and bypass the Fourth Amendment.

To be clear, I do not think any U.S. bills are intended to have this effect. But careful drafting is necessary to ensure that they do not. This should include clear legislative statements that nothing about the new law will change or undermine users' protections from surveillance – in law or in practice. Additional fine-tuning of the legislation, in consultation with surveillance law experts, will also be needed to avoid unintended consequences.

Specifically:

- Any user information that platforms are compelled to share with researchers should not lose the legal protections it currently has under the Fourth Amendment, the SCA, or similar laws.
- By the same token, transparency laws designed to support public research should not create new obligations for platforms to disclose data to the government itself. If lawmakers believe such disclosures are needed, they should be achieved by other means, after open public debate.
- Lawmakers should think carefully about real-world dilemmas that will be encountered by researchers who obtain access to private data. If a researcher believes she sees evidence of a crime, for example, can or should she notify law enforcement? The possibility of information flowing to police in this manner should prompt careful Fourth Amendment

¹⁰ This becomes relevant if, as seems likely, platforms cannot accurately exclude European users from disclosures – although, as discussed in the final section of this testimony, pending legal changes in the DSA may affect this analysis. Under any system, though, obtaining “consent” through unilateral notices to users does not strike me as a real cure. Such notices not only deprive users of the ability to opt out, but risk being either meaninglessly broad, or else so frequent they get ignored.

evaluation, and influence what data researchers see in the first place.¹¹ It should also influence any authority agencies have to approve research that targets individuals or small groups.

- Lawmakers should act with care in requiring platforms to neatly package and deliver information that is nominally public, but that would currently be more difficult to find or assemble. Friction and speed bumps in data collection matter for real-world privacy, and can matter in the law. Under the Fourth Amendment, for example, the fact that activity was carried out in public does not create unlimited license for law enforcement to use sophisticated tools like GPS location-tracking.¹² As a matter of public policy, civil liberties groups have consistently raised concerns about social media monitoring. Organizations like the ACLU have condemned the FBI's acquisition of software for monitoring public social media accounts, for example, as well as the Department of Homeland Security's previous practice of inspecting individuals' social media posts at the border.¹³
- Considerations about users' reasonable expectations of privacy for technically public material online should shape platforms' public transparency reporting obligations. To my mind, those expectations are at their weakest, and transparency is most appropriate, for communications like advertisements or posts from commercial publishers who actively seek public attention. Privacy concerns are much stronger for users whose posts are public simply because they did not understand the privacy settings on a platform like Facebook, or who have no reason to expect attention from anyone but a few people for a public Twitter account. The student who uses Discord to joke with friends about sports, or the LGBTQ+ kid using Reddit to cautiously explore new online communities, should not have to anticipate their every word being preserved under government mandate for future inspection. Such expectations have a documented chilling effect on online speech, and even on users' willingness to search for information on sensitive topics including health or birth control.¹⁴ This chilling effect is not unique to highly private people. As someone with a Twitter following that is approaching PATA's 25,000 threshold for public reporting, I can confidently say that this reporting would change what I say online,

¹¹ This question intersects with evolving case law about the state actor status of private entities that receive information by government mandate. Researchers in this situation could potentially be deemed state actors, meaning that any information they obtain without a warrant may not be admissible in court.

¹² *U.S. v. Jones*, 56 U.S. 400 (2012).

¹³ Aaron Schaffer, *The FBI is spending millions on social media tracking software*, The Washington Post (April 5, 2022), <https://www.washingtonpost.com/politics/2022/04/05/fbi-is-spending-millions-social-media-tracking-software/>; Center for Democracy and Technology, *Fighting Government Intrusions on Privacy and Free Speech at the Border* (2019), <https://cdt.org/2019-annual-report/fighting-government-intrusions-on-privacy-and-free-speech-at-the-border-2019-annual-report/>; Faiza Patel et al, *Social Media Monitoring*, Brennan Center (2020), <https://www.brennancenter.org/our-work/research-reports/social-media-monitoring>.

¹⁴ Alex Marthews and Catherine E. Tucker, *Government Surveillance and Internet Search Behavior* (Feb. 17, 2017), <https://ssrn.com/abstract=2412564>; see also PEN America, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor* (Nov. 12, 2013), <https://pen.org/chilling-effects> (journalists report avoiding writing about terrorism); Jonathon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, Berkeley Technology Law Journal, Vol. 31, No. 1 (2016), <https://ssrn.com/abstract=2769645>.

and prevent me from using the medium as a venue for casual back and forth with the old friends who made up my earliest contacts on the platform.

II. Costs and Competition

Platform transparency has benefits and costs. I am a big believer in the benefits, and have written about them for years.¹⁵ The costs can be harder to spot, but are very real. That's not a reason to forego transparency, but it is a reason to assume a certain "budget" for transparency, and allocate it carefully for maximum public benefit.

Some of the costs are economic. Even tracking platforms' existing content moderation work can come with costs in rebuilding internal tools and expanding and retraining content moderation teams to track data. This can take time away from those teams' other very important priorities, including combating child abuse material or terrorist content online. Collecting expansive new categories of data, like the prevalence metric promoted by Facebook, can be particularly costly.¹⁶ This metric requires quantifying an unknown: the amount of prohibited content that moderators *haven't* found yet. To do so, platforms may use techniques like extrapolating from sample sets evaluated by moderators. Carrying out such evaluation on an ongoing basis, across multiple user languages and diverse cultural contexts, can impose significant costs.

Those costs are particularly meaningful to platforms that cannot, like Facebook or Google, spend billions of dollars on content moderation. This includes platforms that would likely be covered under laws like PATA, based on their number of users.¹⁷ The \$3.7 billion that Facebook has reported spending annually on safety and security, for example, is almost as much as Snap's reported annual revenue,¹⁸ and many times more than Reddit's.¹⁹ It dwarfs the endowment of the non-profit that operates Wikipedia.²⁰ While imposing certain costs may be appropriate, imposing disproportionate ones may have real competitive impact: deterring investment in new platforms, rendering smaller companies less able to attract users, or making them more willing to accept an acquisition offer from an incumbent more capable of meeting these obligations.

¹⁵ See, e.g., Keller and Leerssen, *supra* note 5.

¹⁶ The pros and cons of prevalence as a metric are well discussed in Bradford et al. *Report Of The Facebook Data Transparency Advisory Group* (2019), https://law.yale.edu/sites/default/files/area/center/justice/document/dtag_report_5.22.2019.pdf.

¹⁷ See Appendix I.

¹⁸ Facebook publicly announced that it would spend more than \$3.7bn (c.£2.65bn) on safety and security on the platform in 2019. E&Y, *Understanding how platforms with video-sharing capabilities protect users from harmful content online* (Aug. 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1008128/EYUK-000140696_EY_Report_-_Web_Accessible_Publication_2.pdf. In 2021, Snap recorded \$4.1 billion in revenue. Snap Inc., Form 10-K (2021), retrieved from <https://investor.snap.com/financials/sec-filings/default.aspx>.

¹⁹ Reddit reported \$100 million in quarterly revenue in Q2 2021, implying \$400 million annual revenue. James Vincent, *Reddit is now valued at more than \$10 billion*, The Verge (Aug. 12 2021), <https://www.theverge.com/2021/8/12/22621445/reddit-valuation-revenue-funding-round>.

²⁰ Wikimedia Foundation, *Wikimedia Foundation reaches \$100 million Endowment goal as Wikipedia celebrates 20 years of free knowledge* (Sept. 22, 2021), <https://wikimediafoundation.org/news/2021/09/22/wikimedia-foundation-reaches-100-million-endowment-goal/>.

Other potential costs involve speech and content online. A platform seeking to reduce reporting costs might, for example, adopt simpler, blunter speech rules under its Terms of Service, or simply enforce fewer rules. Efforts to standardize reporting across platforms can, deliberately or not, drive standardization of the underlying speech rules and reduce users' options to participate in diverse speech communities. This homogenizing pressure exists today from advertisers' transparency requests.²¹ U.S. law should not provide similar impetus toward online speech monocultures.²² In particular, lawmakers should be very careful not to prescribe standards based on Facebook that then reshape what their competitors do. It would be perverse if the recent stream of disclosures about Facebook's missteps led to laws inadvertently nudging other platforms closer to Facebook's business model.

Again, none of these concerns are reasons to forego transparency laws. Nor do they all pose questions Congress must answer before enacting transparency laws. Many are appropriate for agency resolution. If lawmakers delegate substantive transparency rules to an agency, they should do so with guidance about the costs to be considered and the benefits to be prioritized in allocating the transparency budget and shaping those rules. In addition to the big picture concerns outlined above, other considerations should include:

- What specific risks are involved in a platform's business? There may, for example, be more legitimate public interest in data about unsafe products on commerce-related sites; copyright infringement on music sites; pornographic or child-inappropriate content on image hosting sites; or disinformation on political discussion sites. The broader and non-risk-specific obligations that may make sense for de facto public forums like YouTube, Twitter, or Tiktok may not make sense for other kinds of Internet giants, like Amazon. They are also hard to justify for platforms where users typically discuss hotel reviews (like Tripadvisor), post software code (like GitHub), or share employment experiences (like Glassdoor). The same analysis may pertain for different parts of one platform. Broad transparency obligation may be harder to justify for Reddit forums about cooking or cats, for example.
- What specific transparency obligations are appropriate, given a platform's size and risk profile? This question should affect researcher data access, with questions of public importance taking priority over more frivolous research. It is also relevant for other kinds of transparency. One example is the ambitious vision in proposals like PATA for ongoing, real-time reporting of sample user content, accompanied by distribution metrics, audience records, and other internal data. Such an expensive undertaking is harder to

²¹ World Federation of Advertisers, *GARM launches its first-ever measurement report for digital brand safety* (Apr. 20, 2021), <https://wfanet.org/knowledge/item/2021/04/20/GARM-launches-its-first-ever-measurement-report-for-digital-brand-safety>.

²² Poorly designed transparency laws can also reduce technical innovation. This might happen, for example, if requirements to report on algorithm changes deterred platforms from experimenting with changes to reduce algorithms' disparate impact or the appearance of harmful content. It might also happen if growing platforms became dependent on vendors providing outsourced moderation and tracking services, and their product design or back-end engineering suffered technical "lock-in" as a result.

justify if it primarily provides better public information about the popularity of restaurant reviews, crafts projects, or Lizzo videos.

- Will a requirement cause platforms to collect user data they otherwise would not?²³ In addition to general privacy issues, this may raise particular concerns if a law causes platforms to collect data on race or other demographic information.
- Will public disclosures give bad or adversarial actors the information they need to game the system, avoiding platforms' mechanisms for fighting spam, coordinated inauthentic behavior, or harassment? This is, I believe, one of the most important concerns to be navigated in transparency proposals.
- Is information competitively sensitive? This may be the case with user traffic data or the details of ranking systems, for example. Some of this information may also currently be protected under trade secret law. Trade secret concerns should not necessarily be a barrier to some disclosures, particularly to researchers with strong confidentiality obligations. That said, vetting and legal obligations will be important in this context, given that academic researchers often move to jobs in the industries they have studied.
- What problems may be caused by disclosing content that platforms have deemed to violate the law or their policies? Researcher access to content is incredibly important, as I have discussed. In many cases even otherwise illegal content, such as material supporting designated foreign terrorist organizations, can and should be lawfully used for research purposes. Other content, such as non-consensual sexual images ("revenge porn," the legal status of which varies by state) seem less appropriate to disclose.
- What degree of precision is needed to support the public purposes of transparency? Given the complexity and risk of error in data collection – particularly for smaller companies – some tolerance for imprecision and revision in reporting may be appropriate. Not every mistake should be a violation of law or carry other drastic legal consequences, in particular the loss of protection under CDA 230.
- Will transparency obligations deter platforms from socially beneficial behavior? A law requiring disclosure of internal research, for example, could discourage platforms from analysis that may ultimately help to protect users or improve products. The same goes for algorithmic transparency mandates. A law requiring disclosure of internal debates over contentious issues could expose employee participants to online abuse or undermine deliberative processes and outcomes.

Again, the point is not that any of these considerations should prevail over transparency priorities. Nor is it that Congress must find a perfect answer to every question. Rather, it is that

²³ For example, in an effort to identify unique users under the PATA Discussion draft's definition of "reach"; demographics under 12(c) and (e); or engagement under the mandatory language at 12(b). Given many public interest advocates' goal of *stopping* platforms from optimizing for engagement, it is odd to require further investment in tracking it.

all of these concerns matter. They should be factors in assessing transparency proposals of all sorts – ranging from public reporting to vetted research to safe harbors for scraping.

III. Speech

Transparency laws are generally intended to improve public access to information. At the same time, they can create other risks to speech rights and the public information environment. I believe that better transparency is essential for wise platform regulation, and hope that well-drafted laws can navigate these risks.

First, as discussed above, is the risk that transparency laws will effectively drive standardization in content policies, and reduce users' options to choose among diverse speech communities. Importantly, this affects *users'* speech rights. If Congressional action effectively reshapes platform speech rules affecting lawful speech, it may be subject to constitutional challenges by users and platforms alike.

The second risk is that transparency laws will be vulnerable to First Amendment challenge by the regulated platforms. This is a major concern. In the case most squarely on point, from 2019, the Fourth Circuit struck down Maryland's disclosure requirements for online campaign ads. The Court cited multiple First Amendment concerns, including chilling effects, compelled speech issues, and insufficient fit between the law's goals and its broad transparency mandates. (Notably, many of the factors listed in the "Costs and Competition" section of this testimony are potentially relevant for these First Amendment questions about means/ends tailoring.) There is also a serious concern about the enforcement of seemingly neutral transparency mandates as a mechanism for state influence on online speech. This is similar to the concern historically raised by many Republicans about the Fairness Doctrine, and has more recently arisen in Twitter's objections to sweeping discovery requests made by Texas Attorney General Ken Paxton.

This is a key question, and not one that has been widely examined. In the only serious public analysis I know of, Santa Clara Law Professor Eric Goldman concludes that transparency mandates raise major First Amendment concerns.²⁴ If I were in the shoes of lawmakers or staff, I would be asking the amazing lawyers at the Congressional Research Service to examine these questions.

IV. CDA 230

Platform transparency obligations should not be tied to platforms' shield from liability for user speech under laws like CDA 230, as is done in some transparency proposals. One reason for this is practical. The data collection and disclosures contemplated by transparency laws are difficult to get right. Errors or disputed interpretations of the law are all but inevitable, even for the most well-intentioned companies. Smaller or less well-resourced companies, or those new to tracking data, are particularly likely to make mistakes – or to reduce and simplify their content

²⁴ Eric Goldman, *The Constitutionality of Mandating Editorial Transparency*, Hastings Law Journal (forthcoming in Vol. 73, 2022), <https://ssrn.com/abstract=4005647>.

moderation efforts in order to avoid liability risk. Transparency regimes should not have this effect, or expose platforms to unpredictable civil liability risk.

For plaintiffs' lawyers and platforms, a rule that caused platforms to lose immunities based on shortcomings in transparency reporting would create a sort of lottery. New opportunities for litigation would vary not based on considered public policy, but based on what transparency mistakes a platform happens to make. A reporting error involving consumer reviews could open the door to litigation by restaurants disputing a customer's online claims; an error involving algorithmic ranking might bring suits about which news sources platforms should prioritize. Platforms would have to litigate even frivolous claims past the motion to dismiss stage, creating incentives to settle improper, opportunistic claims.²⁵

This litigation lottery is not anyone's idea of sensible CDA 230 reform. It would not create procedural avenues for legitimate defamation claims, as the PACT Act does. It would not create remedies for victims of particular and substantial harms, as laws like EARN IT and SESTA/FOSTA attempt to do. It would not limit major platforms' power over public discourse, as proposals from Senator Hawley have aimed to do. Whatever one thinks of any of these bills or their policy goals, they at least reflect considered approaches to addressing specific concerns. Puncturing immunity in response to transparency failings would create more of an arbitrary, shotgun blast approach to public policy.

Involving CDA 230 raises the stakes for transparency laws. It makes the cost of legislative mistakes much higher. Imperfect transparency reporting laws can still do a lot of good; they may not do too much harm; and most of those harms will fall on regulated companies that are comparatively able to advocate for their interests. Flawed approaches to platform immunity laws like CDA 230, by contrast, affect the general public. They can harm ordinary people who often lack the wherewithal to object through lobbying or litigation. One set of harms involves speech and access to information. Platforms concerned for their own liability have reason to simply ban broad swathes of controversial speech or honor inappropriate takedown demands.²⁶ The other harms involve people's economic and social participation. As recent experience has demonstrated, platform purges of speech can also be purges of people, leading to loss of such basic services as payment processing and messaging.²⁷ Transparency laws are not the place to tinker with overall platform immunities and risk such consequences.

²⁵ See discussion of litigation costs in Engine, *Startups, Content Moderation*, & Section 230 (Dec. 9, 2021), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/61b26e51cdb21375a31d312f/1639083602320/Startups%2C+Content+Moderation%2C+and+Section+230+2021.pdf>.

²⁶ James Ball and Paul Hamilos, *Ecuador's President Used Millions Of Dollars Of Public Funds To Censor Critical Online Videos*, BuzzFeed News (Sept. 24, 2015), <https://www.buzzfeednews.com/article/jamesball/ecuadors-president-used-millions-of-dollars-of-public-funds> (describing abuse of legal notices to silence reporting critical of Ecuador's president); Craigslist, *About: FOSTA* <https://www.craigslist.org/about/FOSTA> (describing Craigslist's termination of its online personal ads section in response to SESTA/FOSTA).

²⁷ Danielle Blunt and Ariel Wolf, *Erased—The Impact of FOSTA-SESTA and the Removal of Backpage*, Hacking // Hustling (2020), <https://hackinghustling.org/erased-the-impact-of-fosta-sesta-2020/>.

V. The EU's Approach in the Digital Services Act

The EU's new Digital Services Act (DSA) is a once in a generation overhaul of EU law governing intermediaries' handling of user content. A final version was announced in April 2022, but there is as yet no official draft, and a few details remain unclear. The law extensively regulates platform content moderation, as I described in a recent post.²⁸ Specific obligations vary considerably based on a platform's size and technical functionality.²⁹ Some of the DSA's most far-reaching obligations apply only to "Very Large Online Platforms" or VLOPs, with an EU monthly active user count that exceeds 10% of the EU population. This is currently defined as 45 million people. The equivalent percentage of the U.S. population would be about 33 million people. Attached to this testimony is a rundown of platforms that would likely be caught by various size thresholds.

The DSA includes numerous transparency provisions, many of which have analogs in U.S. proposals. While the final draft may vary in some detail, the basic requirements from earlier drafts are highly likely to persist. These include:

- Public transparency reporting. The DSA requires regular public reports showing aggregate data about content removals, user appeals, and similar issues; information about the number of moderators employed and their training and linguistic expertise; information about the use and claimed accuracy of filters and other automated content moderation tools; and information about monthly active user count. (Arts. 13, 23 and 33)
- Reporting to government about individual content moderation decisions. The DSA obliges platforms to notify users in detail about content moderation decisions that affect them. Copies of these notifications are also to be sent to the European Commission, which intends to include them in a database. (Art. 15)
- Recommender system transparency. Platforms must publish information about their ranking and recommendation systems, including explaining parameters, optimization criteria, objectives, and any options users may have to modify such systems. (Art. 24a, 29). The largest platforms must also "explain the design, logic and the functioning of the algorithms" to regulators upon request.³⁰ (Art. 31)
- Advertising transparency. Platforms must provide information directly in the user interface about the source and targeting of ads. (Art. 24) The largest platforms must also maintain ad archives, accessible via APIs, containing information including the advertisers' identity, the content or "creative" of ads, the dates ads ran, parameters for

²⁸ Daphne Keller, *What Does the DSA Say?*, Stanford Center for Internet and Society Blog (Apr. 25, 2022), <https://cyberlaw.stanford.edu/blog/2022/04/what-does-dsa-say-0>.

²⁹ For a preliminary breakdown of which entities are expected to bear which obligations is here, see Daphne Keller and Jan Jakub Przerwa, *DSA Duties by Entity and Size*, <https://docs.google.com/spreadsheets/d/1rIFtpZmqiW4Vt1IQ54EaJUsk1XGFPzkDdCnLjF-xq3Y/edit#gid=0>.

³⁰ Earlier DSA drafts anticipated an assortment of potential regulatory bodies. In the final draft, most of the regulatory power will sit with the European Commission, but since this is not finalized I refer to "regulators" broadly here.

user group targeting, total users who saw ads broken down by targeted group, and whether each ad was determined to violate law or platform policy. (Art. 30)

- Disclosures to users about content moderation. Platforms must detail their content moderation policies in Terms of Service, and provide information to users affected by moderation decisions as well as to users who report content for violating the law or platform policy. (Art. 12, 14)
- Disclosing internal data to regulators and researchers. Regulators have broad authority to require the largest platforms to disclose internal information regarding their compliance with the DSA overall. Platforms must also give researchers vetted by the regulatory authority with access to information relevant to the platform’s “systemic risks.” A key dispute between DSA negotiators was whether non-academic researchers would be eligible for such access. In all DSA drafts that I’ve seen, regulators are to vet *researchers* rather than *projects*, seemingly meaning that once an entity has been approved, the only real check on its data access arises if platforms formally object. The DSA contemplates future implementing rules to establish technical standards, rules for use of data, and protections for confidential information and security of the service. One of the most complex issues will be the reconciliation of these disclosures with the privacy and data protection provisions of the EU’s General Data Protection Regulation (GDPR). A proposed Code of Conduct for this, from the European Digital Media Observatory, is expected soon.³¹
- Platform risk assessments, risk mitigation plans, audits, and regulatory oversight. The largest platforms regulated under the DSA must conduct annual risk assessments and create risk mitigation plans, as well as undergoing assessment by independent auditors. (Art. 27-28) The resulting reports must be submitted to regulators, and redacted versions must be released publicly. Regulators will also have extensive powers to demand additional information from platforms, perform on-site inspections, and otherwise carry out investigations. (Art. 50-58)

VI. Conclusion

No one likes to come to Congress with a complicated message – especially in the context of legislative changes that are overall positive. But the reality is that transparency reporting is very complicated, and the details matter. Congress is not the right place to sort through all of these details, or to anticipate every technological and economic shift that may reshape transparency needs in the future. It is, however, very much the right place to consider the major policy questions that underlie transparency mandates.

³¹ European Digital Media Observatory, *Launch of the EDMO Working Group on Access to Platform Data* (Aug. 30, 2021), <https://edmo.eu/2021/08/30/launch-of-the-edmo-working-group-on-access-to-platform-data/>.

APPENDIX 1

Reported Monthly Active Usage Data for Content Hosting Platforms
Daphne Keller
April 29, 2022

This document aggregates reported U.S. usage data for certain platforms hosting user-generated content. Some figures are pulled directly from platform SEC filings and public statements, others draw on other public reporting. Extrapolations or assumptions are detailed in the footnotes. **User counts are notoriously unreliable, and different companies may define the metric differently.** Nonetheless, having at least a general idea of user count is important for proposals that would create different legal obligations based on this metric. This brief overview, prepared with the help of an RA, is intended to do that.

More than 25 million monthly active users in the US

Data is either included in, or easily extrapolated from, SEC filings and other platform public statements.

- Facebook: 262M monthly active users in the US & Canada.³²
- YouTube: More than 100M US monthly active users.³³
- Tiktok: More than 100M US monthly active users.³⁴
- Snapchat: More than 97M monthly active users in North America.³⁵
- Wikipedia: More than 97M US monthly active users.³⁶
- Pinterest: 86M US monthly active users.³⁷

³² 2021 Meta 10K, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/14039b47-2e2f-4054-9dc5-71bcc7cf01ce.pdf>. Meta also reports 3.59 billion global monthly active people, which includes users across Whatsapp, Facebook, Instagram, and Messenger. A more recent report suggests still higher figures. Meta, Earnings Presentation Q1 2022, https://s21.q4cdn.com/399680738/files/doc_financials/2022/q1/Q1-2022_Earnings-Presentation_Final.pdf.

³³ YouTube has more than two billion MAU globally. If at least 5% are from the US, then there are at least 100M US MAU. <https://blog.youtube/press/>.

³⁴ TikTok reported 100M US MAU in August 2020, and usage has grown significantly since then. Alex Sherman, "TikTok reveals detailed user numbers for the first time, CNBC. (Aug 24, 2020) <https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html>.

³⁵ Snap currently reports more than 97M daily active users in North America; North America includes Mexico, Canada, Central America. MAU is necessarily higher than DAU. Snap 2021 10K, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001564408/da8288aa-d492-4fd1-b6ce-62dce8206e9f.pdf>.

³⁶ Wikipedia is accessed by 1.95 billion unique devices per month globally. If at least 5% of traffic is from the US, then there are at least 97M MAU from the US. Wikipedia Statistics, "Unique Devices," [https://stats.wikimedia.org/#/all-wikipedia-projects/reading/unique-devices/normal%7Cline%7C2-year%7C\(access-site\)-mobile-site*desktop-site%7Cmonthly](https://stats.wikimedia.org/#/all-wikipedia-projects/reading/unique-devices/normal%7Cline%7C2-year%7C(access-site)-mobile-site*desktop-site%7Cmonthly) (last accessed Apr. 29, 2022).

³⁷ 2021 Pinterest 10K, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001506293/86557168-9b9a-48fc-be82-e9efb7354d2c.pdf>.

- Twitter: More than 38M US monthly active users.³⁸
- LinkedIn: More than 30M US monthly active users.³⁹

Likely more than 25 million monthly active users in the US

Data is estimated based on SEC filings and other platform public statements.

- Wordpress: Likely more than 40M US monthly active visitors.⁴⁰
- Reddit: Likely more than 40M US monthly active users.⁴¹
- Yelp: Likely more than 30M US monthly active visitors.⁴²
- TripAdvisor: Likely more than 30M US monthly active users.⁴³
- Discord: Likely more than 25M US monthly active users.⁴⁴

³⁸ Twitter currently reports 38M US daily active users, and monthly active users is necessarily higher than daily active users. Twitter 2021 10K, <https://d18m0p25nwr6d.cloudfront.net/CIK-0001418091/947c0c34-ca90-4099-b328-a6062adf110f.pdf>.

³⁹ Currently, LinkedIn has 800M global members. <https://about.linkedin.com/>. In 2015 (before Microsoft acquired LinkedIn), LinkedIn reported 98M active monthly users globally. At the time, about 30% of total membership was in the US, so LinkedIn had around 30M MAU US in 2015. This number is likely much higher now, as total membership has doubled since 2015. LinkedIn 2015 10K, <https://www.sec.gov/Archives/edgar/data/1271024/000127102416000035/a20151231-10xkdocument.htm>.

⁴⁰ Wordpress has more than 409 million global visitors each month. If 10% of these users are in the US, then Wordpress has more than 40M monthly US visitors. <https://wordpress.com/activity/>.

⁴¹ In 2018, Reddit had 430M MAU globally, a number that has likely significantly grown since then. If at least 10% of traffic were from the US, then Reddit would have 43M US MAU. Jacob Kastrenakes, "Reddit reveals daily active user count for the first time: 52 million" The Verge (Dec. 1 2020) <https://www.theverge.com/2020/12/1/21754984/reddit-dau-daily-users-revealed>.

⁴² Yelp reports 33M monthly unique app visitors, 45M unique desktop web users, and 56M mobile web unique visitors globally. These numbers are not mutually exclusive. While these numbers are global, Yelp primarily focuses its business in the US and Canada, and so are likely reflective primarily of US users. Yelp 2021 10K, <https://d18m0p25nwr6d.cloudfront.net/CIK-0001345016/6cfb0115-fe02-447b-a835-35393b9e7286.pdf>.

⁴³ In 2019, TripAdvisor had 490M monthly users globally. If at least 6% were from the United States, then TripAdvisor would have 29.4M US MAU. TripAdvisor Investor Relations, "Online Reviews Remain a Trusted Source of Information When Booking Trips, Reveals New Research," (Jul. 16 2019) <https://ir.tripadvisor.com/news-releases/news-release-details/online-reviews-remain-trusted-source-information-when-booking>. Note that monthly usage numbers have fluctuated significantly with the COVID pandemic. The latest 10K stated 2021 usage numbers were 73% of a comparable period in 2019. If current numbers are at 73% of 2019, TripAdvisor would have 357M MAU globally. If 8% are from the US, then it would still have more than 25M US MAU. TripAdvisor 2021 10K, <https://ir.tripadvisor.com/static-files/3e32bcb6-bb03-47ea-bd68-e7a3e82c2d30>.

⁴⁴ Discord reported 150 million monthly active users globally in July 2021. If 17% of these users are in the US, then Discord would have 25.5M monthly active users in the US. Scott Nover, "Once a go-to for gamers, Discord is vying to be a chat app for all," The Verge (July 17, 2021) <https://qz.com/2034087/chat-app-discord-is-shedding-its-gamer-roots/>.

Less than 25 million monthly active users in the US

Data is either included in, or easily extrapolated from, SEC filings and other platform public statements.

- Eventbrite: Less than 25M US monthly active users.⁴⁵
- Bandcamp: Less than 25M US monthly active users.⁴⁶
- Patreon: Less than 8M US monthly active patrons.⁴⁷

Significant platforms for which adequate public data could not be found

This includes data on other platforms for which current US monthly active user data is not available or reasonably inferable. Many platforms on this list may in fact have more than 25 million US MAUs.

Glassdoor: 67M unique monthly users globally.⁴⁸

Vimeo: 260M registered users globally.⁴⁹

Steam: 132M monthly active players globally.⁵⁰

Nextdoor: 35.9M weekly active users globally.⁵¹

Github: 8.32M US monthly visitors in 2015.⁵²

Telegram: 500M active users globally.⁵³

Dropbox: 700M registered users and 16.79M paying users globally.⁵⁴

Etsy: 90.1M buyers and 5.3 million sellers active globally.⁵⁵

Tumblr: no recent public usage data available.

Twitch: no recent public usage data available.

⁴⁵ In 2021, Eventbrite facilitated more than 291M ticket sales globally. On average, this means 24.25M tickets were sold a month. Even if all sales were from unique users, this would mean that Eventbrite would have less than 25M monthly users globally. US usage would likely be significantly lower, as Eventbrite operates in more than 100 countries. Eventbrite 2021 10K, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001475115/210efa34-acc6-4da8-abd1-34c8669239f6.pdf>

⁴⁶ In 2021, Bandcamp users bought 25.75M digital albums, tracks, vinyl records, CDs, cassettes, and t-shirts. If all of these were unique users, then Bandcamp would have 25.75M unique users a year globally; since Bandcamp is used in many countries outside of the US, US usage is very likely below 25M MAU. <https://bandcamp.com/about>.

⁴⁷ Pateron reports 8M monthly active patrons globally. <https://www.patreon.com/about>.

⁴⁸ Glassdoor, “40+ Stats For Companies to Keep In Mind for 2021,” Glassdoor for Employers. <https://www.glassdoor.com/employers/resources/hr-and-recruiting-stats/>

⁴⁹ Vimeo 2021 10K, <https://investors.vimeo.com/static-files/765f2b08-f4bf-4a8b-a625-1b9eae1d6ec>.

⁵⁰ Steam 2021 Year in Review, <https://store.steampowered.com/news/group/4145017/view/3133946090937137590>

⁵¹ Nextdoor 2021 10K, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001846069/c9e1f04e-9b56-4300-ae46-45b7408c9d3b.pdf>

⁵² Usage has likely grown significantly since 2015, but no resources are publicly available to indicate by how much. Brian Doll, “A Closer Look at Europe,” Github Community Blog (June 17, 2015). <https://github.blog/2015-06-17-a-closer-look-at-europe/>.

⁵³ Telegram Twitter Bio, <https://twitter.com/telegram>.

⁵⁴ Dropbox 2021 10K, <https://dropbox.gcs-web.com/static-files/58450624-a3a9-4f41-a94a-8799456275d1>.

⁵⁵ Etsy 2021 10K, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001370637/619701ee-f7dc-4baa-9463-4374cfce885e.pdf>.

APPENDIX 2

Online Platform Transparency Reporting: Research, Laws, Datasets and Policy Proposals
 Daphne Keller
 April 28, 2022

This document, prepared with the help of an RA, is a bibliography aggregating some of the many important sources of information on platform transparency reporting and researcher access to platform data. A primary source was the broader dataset provided by the Partnership for Countering Influence Operations, https://ceip.knack.com/pcio-baseline-datasets#transparency--data-sharing/?view_69_filters=%5B%7B%22field%22%3A%22field_443%22%2C%22operator%22%3A%22contains%22%2C%22value%22%3A%22%22%7D%5D.

Research on Platform Transparency Reporting

- Spandana Singh & Leila Doty, “The Transparency Report Tracking Tool: How Internet Platforms Are Reporting on the Enforcement of Their Content Rules,” New America (2021)
https://d1y8sb8igg2f8e.cloudfront.net/documents/The_Transparency_Report_Tracking_Tool_update_3-18-2021.pdf.
- Spandana Singh and Kevin Bankston, “The Transparency Reporting Toolkit: Content Takedown Reporting,” New America (2018)
<https://www.newamerica.org/oti/reports/transparency-reporting-toolkit-content-takedown-reporting/>.
- UC Berkeley School of Law Human Rights Center, “Digital Lockers: Archiving Social Media Evidence of Atrocity Crimes” (2021)
https://humanrights.berkeley.edu/sites/default/files/digital_lockers_report5.pdf.
- Santa Clara Principles on Transparency, <https://santaclaraprinciples.org/>
- Tech Against Terrorism, “Transparency Reporting Guidelines” (2021)
<https://transparency.techagainstterrorism.org/>.
- Trust and Safety Professional Association, “Transparency Reporting”
<https://www.tspa.org/curriculum/ts-fundamentals/transparency-report/>.
- Facebook, “Charting a Way Forward: Online Content Regulation” (2020)
https://about.fb.com/wp-content/uploads/2020/02/Charting-A-Way-Forward_Online-Content-Regulation-White-Paper-1.pdf.
- Secretary of State for Digital Affairs, “Creating a French Framework to make social media platforms more accountable: Acting in France with a European vision,” (2019)
https://www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf (pgs 20, 25, 26 discuss proposed regulation including a transparency requirement for ranking and content moderation).

- OECD, “Transparency reporting on terrorist and violent extremist content online: An update on the global top 50 content sharing services”, OECD Digital Economy Papers, (2021) <https://doi.org/10.1787/8af4ab29-en>.
- European Data Protection Supervisor, “A Preliminary Opinion on Data Protection and Scientific Research,” (2020) https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.
- Integrity Institute, “Ranking and Design Transparency: Data, Datasets, and Reports to track Responsible Algorithmic and Platform Design,” (2021) <https://static1.squarespace.com/static/614cbb3258c5c87026497577/t/617834ea6ee73c074427e415/1635267819444/Ranking+and+Design+Transparency+%28EXTERNAL%29.pdf>.
- Amelia Pia Heldt, “Reading Between the Lines and the Numbers: An Analysis of the First NetzDG Reports,” (2019) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3413677.
- Robert Gorwa and Timothy Garton Ash, “Democratic Transparency in the Platform Society, chapter in Social Media and Democracy: The State of the Field,” (2020) <https://osf.io/preprints/socarxiv/ehcy2/>.
- Daphne Keller, “Some Humility about Transparency,” The Center for Internet and Society (2021) <http://cyberlaw.stanford.edu/blog/2021/03/some-humility-about-transparency>.
- Svea Windwehr and Jillian C. York, “Thank You For Your Transparency Report, Here's Everything That's Missing,” EFF (2020) <https://www.eff.org/deeplinks/2020/10/thank-you-your-transparency-report-heres-everything-thats-missing>.
- Mark MacCarthy, “Transparency Requirements for Digital Social Media Platforms: Recommendations for Policy Makers and Industry,” Trans Atlantic Working Group (2020) https://www.ivir.nl/publicaties/download/Transparency_MacCarthy_Feb_2020.pdf.
- Relevant laws:
 - Australian Code of Practice on Disinformation and Misinformation, Transparency Reports <https://digi.org.au/disinformation-code/> (2021).
 - Canada Bill C-76, 2018 <https://www.parl.ca/LegisInfo/en/bill/42-1/C-76>. (social media platforms must create and publish archives of election and partisan ads).
 - European Parliament and Council of the European Union, Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, Article 7 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.172.01.0079.01.ENG&toc=OJ%3AL%3A2021%3A172%3AATOC (requiring companies to report on removing terrorist content).

- French National Assembly, "La Lutte Contre la Manipulation de l'Information" <https://www.gouvernement.fr/action/contre-la-manipulation-de-l-information> (requiring reporting on ads).
- German Network Enforcement Amendment Act, <https://perma.cc/7UCW-AA3A> (requiring reporting on content enforcement)
- India Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf (requiring reporting on enforcement actions).

Researcher Access to Data

- Caitlin Vogus, "Independent Researcher Access to Social Media Data: Comparing Legislative Proposals," Center for Democracy and Technology (Apr. 2022) <https://cdt.org/insights/independent-researcher-access-to-social-media-data-comparing-legislative-proposals/>.
- Caitlin Vogus and Emma Llansó, "Report – Making Transparency Meaningful: A Framework for Policymakers," Center for Democracy and Technology (Dec. 14, 2021) <https://cdt.org/insights/report-making-transparency-meaningful-a-framework-for-policymakers/>.
- Drs. Amy O'Hara and Jodi Nelson, "Evaluation of the Social Science One – Social Science Research Council – Facebook Partnership," Hewlett Packard (2019) <https://hewlett.org/wp-content/uploads/2020/02/Facebook-Partnership-Final-Evaluation-Report.pdf>.
- Zuckerman et. al, "New Approaches to Platform Data Research," NetGain Partnership (2021) <https://www.netgainpartnership.org/resources/2021/2/25/new-approaches-to-platform-data-research>.
- Gary King and Nathaniel Persily, "A New Model for Industry-Academic Partnerships" PS: Political Science and Politics, 53, 4, Pp. 703-709. Copy at <https://tinyurl.com/ybqrtrsz> (2019).
- Axel Bruns, "After the 'APIcalypse': social media platforms and their fight against critical scholarly research," Information, Communication & Society, 22:11, 1544-1566, DOI: 10.1080/1369118X.2019.1637447 (2019).
- Jef Ausloos, Paddy Leerssen, Pim ten Thije, "Operationalizing Research Access in Platform Governance: What to learn from other industries," (June 2020) https://www.ivir.nl/publicaties/download/GoverningPlatforms_IViR_study_June2020-AlgorithmWatch-2020-06-24.pdf.
- Creating a Platform for the Sharing of Sensitive Online Data: White Papers. <https://securelysharingdata.com/whitepapers.html> (Includes several papers. The proposed "Institute for the Secure Sharing of Online Data" (ISSOD) is a new initiative that aims to establish an institute to: (a) act as a data repository for large-scale social and digital

media data sets (b) provide a replication archive for large sensitive scale social and digital media datasets (c) establish a new “National Information Survey” that provide regular surveys to monitor trends in digital information consumption).

- Stanford HAI, “Building a National AI Research Resource: A Blueprint for the National Research Cloud” (2022) https://hai.stanford.edu/sites/default/files/2022-01/HAI_NRCR_v17.pdf.
- French Ambassador for Digital Affairs, “Facebook Ads Library Assessment” (2020) <https://disinfo.quaidorsay.fr/en/facebook-ads-library-assessment>.
- Mozilla, “Facebook and Google: This is What an Effective Ad Archive API Looks Like” (March 2019) <https://blog.mozilla.org/en/mozilla/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like/>.
- Daphne Keller and Paddy Leerssen, “Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation” (Dec. 2019) <https://www.semanticscholar.org/paper/Facts-and-Where-to-Find-Them%3A-Empirical-Research-on-Keller-Leerssen/d7f89602d821a724a007375bd8ee4382b9930eaf?p2df>.
- Association of Internet Researchers, “Internet Research: Ethical Guidelines 3.0,” (2019) <https://aoir.org/reports/ethics3.pdf>.
- Microsoft and NYU Open Data Policy Lab. <https://opendatapolicylab.org/> (Institute for enabling access to public and private data)
- Marco Gaboardi, James Honaker, Gary King, Jack Murtagh, “PSI: a Private data Sharing Interface,” (2016) <https://arxiv.org/abs/1609.04340>.
- Brandie Nonnecker and Camille Carlton, “EU and US legislation seek to open up digital platform data,” *Science* (Feb 2022). <https://doi.org/10.1126/science.abl8537>.
- Data currently available for researchers:
 - Facebook Ad Targeting Transparency Data Sets, <https://research.facebook.com/blog/2021/02/introducing-new-election-related-ad-data-sets-for-researchers/>.
 - Facebook and Instagram Research Initiative on US 2020 Presidential Election, <https://about.fb.com/news/2020/08/research-impact-of-facebook-and-instagram-on-us-election/>.
 - Solom Messing, Saurav Mahanti, Christina DeGregorio, Zagreb Mukerjee, Bogdan State, Bennett Hillenbrand, Chaya Nayak, Arjun Wilkins, Gary Kings, Nathaniel Persily, “Facebook Privacy-Protected Full URLs Data Set”: https://solomonmg.github.io/pdf/Facebook_DP_URLs_Dataset.pdf (exposure data for widely-shared URLs).
 - Facebook Data for Good, <https://dataforgood.facebook.com/dfg/about> (data sharing with non-profits)
 - LinkedIn and World Bank Group, “Industry Jobs and Skills Trends,” <https://linkedindata.worldbank.org/>.

- Microsoft and ODI Open Data Campaign, <https://theodi.org/project/microsoft-and-the-odi-helping-bridge-the-data-divide/>.
- NYU Political Ad Collector and Observer, <https://engineering.nyu.edu/news/new-tool-analyze-political-advertising-facebook-reveals-massive-discrepancies-party-spending>.
- Surya Mattu, Leon Yin, Angie Waller, and Jon Keegan, “How We Built a Facebook Inspector, *The Markup* (Jan. 2021) <https://themarkup.org/citizen-browser/2021/01/05/how-we-built-a-facebook-inspector>
- Mozilla, “Getting serious about political ad transparency with Ad Analysis for Facebook,” (Feb. 2019) <https://blog.mozilla.org/netpolicy/2018/10/18/getting-serious-about-political-ad-transparency-with-ad-analysis-for-facebook/>.
- Rally Mozilla, <https://rally.mozilla.org/> (allows you to “donate” your data to researchers).
- Twitter Archive at the Library of Congress, <https://blogs.loc.gov/loc/2017/12/update-on-the-twitter-archive-at-the-library-of-congress-2/>.
- Twitter Academic Research Product Track, <https://developer.twitter.com/en/products/twitter-api/academic-research> (provides enhanced data access for researchers).

Testimony of Professor Nathaniel Persily

James B. McClatchy Professor of Law

Co-Director of the Stanford Cyber Policy Center

Stanford Law School¹

Before the United States Senate Committee on the Judiciary

Subcommittee on Privacy, Technology, and the Law

“Platform Transparency: Understanding the Impact of Social Media”

Submitted May 2, 2022

Thank you, Mr. Chairman and Members of the Committee, for inviting me today to testify on the need for greater transparency from the internet platforms. My name is Nate Persily. I am the James B. McClatchy Professor of Law at Stanford Law School and Co-Director of the Stanford Cyber Policy Center. Perhaps most notably for purposes of this hearing, I was also the cofounder of Social Science One, an effort to get internet platforms, such as Facebook, to share privacy-protected data with outside researchers.

I want to use my remarks today to explain the purposes greater transparency serves, the types of transparency that are necessary, and the reason that only

¹ Affiliation for identification purposes only; appearing in personal capacity.

governmental regulation – not voluntary efforts by the companies – can ensure the benefits of transparency while protecting user privacy. **We cannot live in a world where Facebook and Google know nearly everything about us, and we know next to nothing about them. These platforms have lost their right to secrecy, and it is well past the time that someone other than the firms’ own data scientists be granted access to the data that reveal the impact of these platforms on the information ecosystem.**²

It has become fashionable recently to describe these platforms as the global public square. I happen to disagree with that characterization, because these platforms, by design, organize and prioritize some kinds of communication over others and structure their environments to create a specific user experience. If anything, the internet itself is the public square, whereas the platforms are privately controlled spaces with specific rules for interaction. For those to whom the metaphor appeals, however, it usually is in service of an argument that these platforms should be more open and less censorious in their content moderation. That debate is important to have, and we should hope that different platforms adopt different algorithms and content moderation rules so that the

² For an expanded version of the arguments presented here, see Social Media Platforms and the Amplification of Domestic Extremism and Other Harmful Content: Hearing before the United States Senate Committee on Homeland Security and Governmental Affairs, Oct. 28, 2021 (testimony of Nathaniel Persily); Nathaniel Persily, “A Proposal for Researcher Access to Platform Data: The Platform Transparency and Accountability Act,” 1 *Journal of Online Trust and Safety* (2021), <https://doi.org/10.54501/jots.v1i1.22>; Nathaniel Persily & Joshua A. Tucker, *How to fix social media? Start with independent research*, Brookings Inst., Dec. 1, 2021, <https://www.brookings.edu/research/how-to-fix-social-media-start-with-independent-research/>; Nathaniel Persily, Opening a Window Into Tech: The Challenge and Opportunity for Data Transparency, Stanford Cyber Policy Center (2020), available at https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/cpc-open_windows_np_v3.pdf; Nathaniel Persily & Joshua A. Tucker, “Conclusion: The Challenges and Opportunities for Social Media Research,” in *Social Media and Democracy: The State of the Field and Prospects for Reform* (N. Persily & J. Tucker eds., 2020).

online marketplace of ideas can be a true market where users can “vote with their clicks” to opt into different sets of rules.

Whatever one might say of the metaphor, both the enforcement of the rules that govern the public square and the behavior of speakers within it should be transparent. In this respect, the large platforms fall short. The public does not have a window into the dynamics of speech regulation in these critically important spaces or how content spreads within and across them. The role of law in this area, at the very least, is to make the public square genuinely public: to allow for outsiders to have the same understanding as insiders with respect to how these platforms operate.

I. The Goals of Transparency

In discussions of potential platform regulations, transparency proposals are often viewed as less significant than other kinds of interventions, such as reforms of Section 230 of the Communications Decency Act. That assessment, however, understates the foundational role that transparency can play in a larger regulatory regime and how regulated industries adapt based on the information they are forced to disclose. Transparency proposals, such as the Platform Accountability and Transparency Act, will lead to fundamental change at the platforms, while at the same time educating policymakers considering other forms of tech regulation.

First and most important, greater transparency will affect the behavior of the firms themselves. When the platforms know that they are being watched and that outsiders will

have access to the same data as insiders, they will inevitably change their policies and enforcement of them. Forcing disclosure means that content moderation or algorithmic manipulation cannot happen in the dark without consequences. Under a regime such as that proposed in PATA, the public will routinely be made aware of changes in policies and practices related to advertising, content moderation, and algorithmic design. If a platform's policies or affordances are responsible either for propagation of dangerous content or for undue censorship, the platform will not be able to hide it from public view.

Second, transparency is critical for the creation of good public policy. At present there are fundamental disagreements between outsiders and insiders as to the scale of online harms and the responsibility of the platforms for causing or amplifying them. Critics focus on the number of posts (or related likes or reposts) of problematic content (disinformation, hate speech, etc.), whereas platform defenders tend to argue that such content is a tiny share of the average user's feed. Moreover, it is now part of conventional wisdom that the algorithms and recommendation engines (let alone advertising) of the major platforms routinely amplify hate speech, disinformation, and other problematic content. However, most of the academic investigation of these topics suggests it is more common for people to seek out this problematic content rather than have it force-fed to them. If Congress or any legislature around the world is to make policy with respect to online content, it is critical that we have answers to these questions. We can only get answers if outsiders are given access to the same data from which the platform advocates draw their conclusions.

Third, the public has a right to know how these platforms operate and the scale and character of online harms. Much, if not most, of human interaction is now occurring

through digital communication. It has become fashionable to describe these platforms as information monopolies, usually in service of an antitrust argument about the dangers of concentrated power over critical speech forums. But these platforms are information monopolies in a different sense: they, and they alone, hold the keys to the data that is most informative as to contemporary society. Not only are outsiders largely in the dark about the role that platforms play in exacerbating social problems, but the principal information about society itself is now in a few private hands. If we want to understand pretty much any contemporary problem – e.g., the dynamics of the pandemic, the causes and scale of teenage depression, the challenges to journalism, the depths of political polarization, foreign election interference – we need to have access to data that are locked up in these private companies. In short, transparency is about more than looking over the shoulders of the platforms; it is a necessary predicate to understanding most contemporary policy challenges “in the real world” as well.

II. Transparency for Whom and About What?

Transparency, like all values related to regulation of the information ecosystem, comes with tradeoffs. Unfettered transparency could lead to violations of user privacy, as well as gamesmanship by bad actors seeking to outflank platform countermeasures designed to protect users. The goal of platform transparency legislation should be to make public all that can be made public without compromising user privacy and without providing the tools for adversaries to game the platforms’ rules and algorithms. As with any regulatory challenge, transparency can be done well or poorly, and it is the role of policy to confront these tradeoffs honestly with the goal of maximizing the benefits of transparency (outlined above) while minimizing its costs.

The proposed Platform Accountability and Transparency Act (PATA) seeks to do just that. Like any draft legislation, it is not perfect and needs refinement.³ But it goes farther and provides more detail than any previous efforts. Most critically, it focuses on what I consider to be three legs to the transparency stool: (1) broad obligations for public disclosures; (2) protection for researchers analyzing publicly available data; and (3) supervised access for vetted researchers to the data accessible to the platforms own data scientists.

PATA requires large platforms to issue public reports or representative data on several critical topics. It gives the Federal Trade Commission power to require reports on widely shared content, including metrics for engagement and reach, as well as disclosure of the types of datasets in the platform's possession related to users or content. The proposal also requires the disclosure of advertising data, including the identity of advertisers, the ad content itself, and information as to targeting and reach. Finally, it requires disclosures related to algorithms and metrics: in particular, a summary of the inputs to the algorithms and the "optimization objective of such models."

Second, PATA immunizes researchers from civil and criminal liability for scraping of non-private data from platforms, if they meet a number of specified requirements. This provision responds to the controversy sparked by the NYU Ad

³ In her submitted testimony, my colleague, Daphne Keller, highlights some areas of PATA in need of refinement. I agree with most of her arguments. However, all of these objections can be satisfied with modifications that do not undermine the critical requirements of the largest platforms to provide broad public disclosures, access of vetted researchers to platform data, and civil and criminal immunity for researchers doing public interested work on public platform data. One point of hers that I would like to stress is the importance of limiting these transparency obligations to the largest platforms – namely, Facebook/Meta, Google/YouTube, TikTok, and Twitter. We do not want the transparency obligations to inhibit the rise of potential competitors to these platforms or to place excessive burdens on small platforms that might be forced to shut down were they forced to comply.

Observatory's efforts to study Facebook advertising.⁴ Researchers there provided a browser plugin to volunteers with Facebook accounts to capture information about the ads that the platform served to them. Citing concerns about privacy arising from its settlement with the FTC following the Cambridge Analytica scandal, Facebook disabled the accounts of the NYU researchers. Afterwards, the FTC took the extraordinary step of clarifying that the settlement did not prevent Facebook from allowing such researcher access. The sordid saga concerning the Ad Observatory only further reinforces the need for law to give direction as to what kinds of research are permitted or forbidden on these large platforms. Despite some recent court decisions in their favor, researchers continue to avoid pursuing certain projects for fear that they might be prosecuted or held liable under the Computer Fraud and Abuse Act.

Third, PATA provides a secure pathway for vetted researchers to gain access to data already in the firm's possession, which otherwise might only be analyzed by the firm's own data scientists. Some data, even in aggregated and anonymized form, might be too sensitive to be made public. A secure pathway for vetted researchers, with safeguards to protect the privacy of that information, is absolutely critical to answering the most pressing questions concerning the impact of platform policies on the information ecosystem.

Although the public reporting requirements will be quite useful to understanding certain phenomena, only secure access will allow research on "who" has seen/engaged with "what," "when," and "why." These are the critical inquiries undergirding any

⁴ Laura Edelson & Damon McCoy, "We Research Misinformation on Facebook. It Just Disabled Our Accounts," *New York Times*, Aug. 10, 2021.

analysis of social media phenomena. Researchers do not need to analyze individual accounts – and indeed, they should be criminally punished if they try to do so. However, they need to understand which large demographic groups (age, race, gender, region, etc.) have engaged with which types of content (organic content, media, advertising etc.). They also need to understand when they have done so (e.g., in the period just before an election, after a major event, or in the normal pace of the platform) and “why” (for example, was the content referred to them by a recommendation or algorithmic system or did they search for it?).

If we had access to platform information along the three paths described above, what might we learn? Renée DiResta, Laura Edelson, Brendan Nyhan, and Ethan Zuckerman recently published some examples of the questions that could be asked and answered in an article in *Scientific American* titled “It’s Time to Open the Black Box of Social Media” (Apr. 28, 2022):

- Research suggests that misinformation is often more engaging than other types of content. Why is this the case? What features of misinformation are most associated with heightened user engagement and virality? Researchers have proposed that novelty and emotionality are key factors, but we need more research to know if this is the case. A better understanding of why misinformation is so engaging will help platforms improve their algorithms and recommend misinformation less often.
- Research shows that the delivery optimization techniques that social media companies use to maximize revenue and even ad delivery algorithms themselves can be discriminatory. Are some groups of users significantly more likely than others to see potentially harmful ads, such as consumer scams? Are others less likely to see useful ads, such as job postings? How can ad networks improve their delivery and optimization to be less discriminatory?
- Social media companies attempt to combat misinformation by labeling content of questionable provenance, hoping to push users

towards more accurate information. Results from survey experiments show that the effects of labels on beliefs and behavior are mixed. We need to learn more about whether labels are effective when individuals encounter them on platforms. Do labels reduce the spread of misinformation or attract attention to posts that users might otherwise ignore? Do people start to ignore labels as they become more familiar?

- Internal studies at Twitter show that Twitter’s algorithms amplify right-leaning politicians and political news sources more than left-leaning accounts in six of seven countries studied. Do other algorithms used by other social media platforms show systemic political bias as well?
- Because of the central role they now play in public discourse, platforms have a great deal of power over who can speak. Minority groups sometimes feel their views are silenced online as a consequence of platform moderation decisions. Do decisions about what content is allowed on a platform affect some groups disproportionately? Are platforms allowing some users to silence others through the misuse of moderation tools or through systemic harassment designed to silence certain viewpoints?

Different people prioritize different questions when it comes to the platforms. Some worry about the scale and character of online harms, such as hate speech, disinformation, incitement and child endangerment. Others worry that the platforms are engaging in undue censorship, perhaps tilting the speech marketplace toward a particular ideology or party. Transparency and outsider access to platform data respond to both of those concerns. Indeed, while the political parties may diverge with respect to the other forms of tech regulation they support, greater transparency to reveal the nature of online harms and the ways that platforms are responding to them represents a bipartisan first step on the road to sound policy supported by either side.

III. Why Government Regulation Is Necessary

In an ideal world, the platforms, on their own, would make the data described above available for outside analysis. To be fair, some significant exceptions exist to the general rule of platform data hoarding. Twitter has established relationships with a range of academics to provide access to real-time and historical Twitter data⁵ and have provided curated datasets on influence operations. Facebook worked with Social Science One (described below), acquired and promoted CrowdTangle (a platform that allows for analysis of public posts), and has recently teamed up with a large group of independent social media researchers to analyze the impact of the platform on the 2020 election.⁶ To my knowledge, neither Google nor TikTok have embarked on similar efforts, although some individual academics have gotten favored access to all of these platforms, sometimes with a requirement of pre-publication review of research.⁷

We cannot and should not depend on the generosity of platforms, however, for analysis of data in the public interest. Indeed, we tend to forget that the data they hold is, in the end, about us, the users. Analysis of our behavior and communication – especially when it has profound civic consequences – should not be the sole province of the firm’s

⁵ See Twitter API, Academic Research Access, at <https://developer.twitter.com/en/products/twitter-api/academic-research#:~:text=New%20and%20existing%20Twitter%20developers,an%20academic%20institution%20or%20university>.

⁶ See Nick Clegg & Chaya Nayak, New Facebook and Instagram Research Initiative to Look at US 2020 Presidential Election, Aug. 31, 2020, <https://about.fb.com/news/2020/08/research-impact-of-facebook-and-instagram-on-us-election/>; Talia Stroud, Joshua A. Tucker, Annie Franco, & Chad P. Kiewiet de Jonge, A Proposal for Understanding Social Media’s Impact on Elections: Rigorous, Peer-Reviewed Scientific Research, Aug. 31, 2020, https://medium.com/@2020_election_research_project/a-proposal-for-understanding-social-medias-impact-on-elections-4ca5b7aae10.

⁷ For a survey of existing and proposed approaches to platform data sharing, see Elizabeth Hansen Shapiro, Michael Sugarman, Fernando Bermejo, & Ethan Zuckerman, *New Approaches to Platform Data Research* (Feb. 2021); Jacob N. Shapiro, Natalie Thompson, & Alicia Wanless, *Research Collaboration on Influence Operations Between Industry and Academia: A Way Forward*, Carnegie Endowment for International Peace, Dec. 2020, https://carnegieendowment.org/files/Shapiro_Thompson_Wanless_Instantiating_Models_final.pdf.

employees, who are inexorably tied to the profit maximizing mission of the firm.

Platform data scientists are restricted in the questions they can ask of the data and usually prevented from releasing their findings to the outside world. Although every effort must be undertaken to protect user privacy, some independent actors must have access to the data under the firm's control.

This was the motivation for the creation of Social Science One, an effort to provide independent researchers with access to platform data. Social Science One was run by academics for academics, and was independently funded by a set of foundations. Researchers and their projects were vetted by the Social Science Research Council; Facebook played no role in approving either researchers or research projects.

Facebook's principal role was, at the inception and to this day, to provide datasets for analysis by these vetted academics. To Facebook's credit, the project did produce one of the largest social media datasets in existence, which has been analyzed by close to one hundred researchers and is updated every few months. That dataset includes URLs (shared publicly at least 100 times) with certain categories of engagement data attached, to enable researchers to get a rough sense of which URLs were seen or engaged with by which large categories of users (by age, gender, and region). We had hoped to provide a much richer dataset akin to those required by PATA with the URLs dataset constituting a step in that direction.

Social Science One faced two sets of problems almost from its inception. The first and most significant was concern over protecting privacy. Within weeks of the announcement of Social Science One, the Electronic Privacy Information Center (EPIC)

filed a “cease and desist” letter with the Federal Trade Commission and the European Union Data Protection Board. EPIC alleged that the research effort, by its very nature, violated user privacy and therefore violated both the General Data Protection Regulation of the European Union and the 2011 consent decree Facebook entered into with the FTC.

EPIC’s letter raised the Cambridge Analytica scandal as a reason that academics should not be granted access to platform data. The cloud cast by the Cambridge Analytica scandal over Social Science One (and parallel research efforts) cannot be overstated. That scandal involved an academic’s misuse of social graph data and its concomitant transfer to the international political consulting firm, Cambridge Analytica, which allegedly used it and other data to develop profiles for voter targeting. Later the FTC settled with Facebook, which paid \$5 billion dollars to end the dispute, roughly a year into the existence of Social Science One. The scandal revealed how much data is in the possession of these platform, but it also now serves as a clarion call for the establishment of a legally sanctioned and regulated process that will simultaneously grant researcher access while ensuring government oversight to protect user privacy.

These pressures regarding user privacy constrained Social Science One as it tried to realize independent researchers’ hopes of broad data access. Statistical noise, following the principles of differential privacy, was added to the URLs dataset, described above. In other words, even though the data were aggregated at the URL level (that is, no individual level data appeared in the dataset) and only URLs that were shared 100 times were included, nevertheless Facebook felt it necessary to remove any risk that someone might somehow figure a way to break down the aggregated data to surmise what a given individual may have seen on the platform. I continue to disagree that such a strategy was

legally necessary to protect privacy, but these were sincerely held concerns that stymied many of our efforts to establish a system for independent analysis of platform data.

The second challenge that Social Science One confronted concerned the reliability of the data that Facebook delivered. Although it came to light after I resigned as co-chair of Social Science One, Facebook data scientists discovered that the URLs dataset neglected to include about a third of the United States population in the available data. In particular, the dataset did not include users for whom Facebook had not identified a political affinity, thereby likely leaving out of the URL interaction data many political moderates and others whose political views were not easily classified. Once the error was detected, Facebook updated the data within a month, but some papers that had used the data had already been published.

The experience of Social Science One is instructive as we consider legislative options to require platforms to share data with outside researchers. Until there is a countervailing legal requirement that pushes firms to share data, they will always perceive the costs of granting access as exceeding the benefits. Moreover, the life-cycle of Social Science One highlights how critical it is to do as much as possible to protect and safeguard user privacy in the design of these new data sharing initiatives. Only national legislation that creates a system of federal oversight that compels access to data under strict privacy protections can serve as a pathway both to providing the necessary information the public deserves and to respecting the public's legitimate expectations of privacy.

Conclusion

Greater transparency for the large internet platforms is that rare form of tech regulation that should appeal to both Republicans and Democrats. Whether one is most concerned about the scale of disinformation and extremism on the platforms or the platforms' potential bias in moderating content, greater access to platform data represents a prerequisite to gathering evidence and crafting public policy in this domain. It might take years for the parties to come together on regulation related to content moderation, antitrust, privacy, and online advertising. In the meantime, it is critical – now – to set up a data sharing regime that can allow policymakers and the public alike to understand how new digital technologies are affecting society.

If the United States does not act, Europe will. The new Digital Services Act provides for a series of public disclosures and data-sharing efforts. A working group from the European Digital Media Observatory (EDMO)⁸ will soon release its code of conduct on researcher access to platform data. Greater transparency seems inevitable at this point. The question is which government will take the lead and how comprehensive legally compelled transparency will be.

In the span of less than a decade, what had been a widely shared utopian view of the potential of digital technologies for democracy has turned decidedly apocalyptic. Previously heralded as giving voice to the voiceless, the platforms are now blamed for worsening public health crises, teen depression and suicide, election-related conspiracies,

⁸ See European Digital Media Observatory, Launch of the EDMO Working Group on Access to Platform Data, Aug. 31, 2021, <https://edmo.eu/2021/08/30/launch-of-the-edmo-working-group-on-access-to-platform-data/>.

ideological censorship, political polarization, and even genocide. All of this might be true. Until the platforms disclose more information to the public and subject themselves to outside, independent oversight, we will not be able to understand the prevalence of these problems or the responsibility of the platforms for exacerbating them.

Testimony of Brandon Silverman to the Subcommittee on Privacy, Technology, and the Law (Senate Judiciary Committee)

Hearing: Platform Transparency: Understanding the Impact of Social Media

May 4th, 2022

Introduction

My name is Brandon Silverman, and for over ten years, I was the CEO and co-founder of CrowdTangle, a social media analytics tool acquired by Facebook in 2016.

Our mission was to help make Facebook the most transparent social media company in the world, and we were very good at what we did. By the end of 2020, the New York Times called us "perhaps the most effective transparency tool in the history of social media."¹ However, in the spring of 2020, after an intense internal debate, Facebook paused all work on CrowdTangle and disbanded the team running it. I left the company shortly thereafter. Today, the future of CrowdTangle is up in the air, and along with it, one of the most robust and successful real-time transparency programs that Facebook operates.

I've worked with data from almost every major social media platform from Vine to Twitter to YouTube to Instagram. I've seen how tens of thousands of researchers, journalists & activists can use social media data to protect our elections, prevent real-world violence, fight global pandemics, empower independent journalists, hold platforms accountable, and more. And I've worked on transparency from inside one of the largest platforms in the world.

I'm here today to share my story, what I experienced first-hand, and ultimately why I believe it's time to stop sitting back and hoping that platforms voluntarily share data and instead pass legislation that makes data sharing mandatory for the entire industry.

Our Story

When CrowdTangle started, we were a social media analytics tool that made it easy for publishers to understand what was happening on social media. We made it easy to see what stories were going viral, track influencers, stay on top of trends, and more.

In 2016, we were acquired by Facebook², and I spent four years leading the CrowdTangle team while there. For a while, being inside Facebook gave us a powerful home that supercharged our work to help publishers and news outlets. Our team tripled in size; we launched dozens of new features and expanded the team internationally.

In 2018, we underwent an important shift: instead of just trying to support publishers, we began focusing on a new mission of making Facebook the most transparent social media platform in

¹ <https://www.nytimes.com/2022/01/02/business/media/crowdtangle-facebook-brandon-silverman.html>

² <https://www.theverge.com/2016/11/11/13594338/facebook-acquires-crowdtangle>

the world. We expanded our work to more and more industries, including academia³. Our data was the basis of hundreds of academic research papers, including in *Nature*⁴, *Science*, as well as referenced in thousands of news articles by journalists around the world reporting on social media. Our insights were referenced in Congressional testimony, used by human rights organizations in developing countries and lauded by Facebook's executives. We became one of the most widely used tools in the world to understand and see what was happening on social media in real-time and there was no shortage of use cases.

The Power of Transparency

Unless you've spent time trying to study social media, it can be hard to understand what transparency actually looks like in practice and why it's so hard right now.

When it comes to the type of transparency we focused on at CrowdTangle, one way to think about it is to imagine television except with two big differences. There are no any ratings and instead of having 3 or 4 prominent news shows, there were hundreds of thousands of channels broadcasting news live at any given moment. If you were interested in studying a medium like that and you wanted to know what was the largest broadcast on any given night, who the most influential host was, what the biggest story of the day was or what was being said about COVID, it would be impossible. If you wanted to study that information ecosystem and understand how it might be shaping and influencing our society, it would be impossible. That's essentially how social media functions unless platforms voluntarily decide to make that data available.

Our goal at CrowdTangle was to make all that information accessible and incredibly easy to use for as many social platforms as we could possibly work with. At one point, we had integrations with Facebook, Instagram, YouTube, Vine, Twitter, and Reddit. As a result, we saw more use cases than we ever imagined, including:

- We worked with hundreds of local news outlets to help them report on and monitor social media in their local communities⁵.
- In 2020, we worked with every single local election board across the US to help them monitor for misleading voting information⁶ and have it taken down from the platform.
- In the Philippines, our tool helped Rappler and this year's Nobel Peace Prize Winner Maria Ressa's team identify accounts violating Facebook's terms of service and spreading disinformation in the lead-up to national elections⁷.
- When COVID took off, we made public versions of CrowdTangle available in almost every country in the world⁸ so that local communities could monitor the public discussion about the pandemic.

³ <https://wersm.com/facebook-opens-up-crowdtangle-to-academics-and-researchers/>

⁴ <https://www.nature.com/articles/s41599-020-0452-1>

⁵ <https://www.adweek.com/performance-marketing/crowdtangle-for-local-news/>

⁶ <https://about.fb.com/wp-content/uploads/2020/02/Helping-to-Protect-the-US-2020-Elections.pdf>

⁷ <https://www.rappler.com/newsbreak/investigative/245290-marcos-networked-propaganda-social-media/>

⁸ <https://www.facebook.com/gpa/blog/launching-crowdtangle-covid-19-vaccine-live-displays>

- We helped public interest, and advocacy organizations like Avaaz hold platforms accountable⁹ for their public commitments to elections, misinformation, COVID, and more.
- We partnered with hundreds of fact-checking organizations around the world¹⁰, including the International Fact-checking Network, and became a critical part of their effort to identify & respond to misinformation in real-time.
- We helped researchers uncover inauthentic networks and help them get removed from the platform as quickly as possible, including Russian-linked influence operations in Africa¹¹ and more.
- In developing countries like Myanmar, Ethiopia, and Sri Lanka, we helped human rights organizations like the Myanmar Accountability Network¹² protect the integrity of elections and help prevent real-world violence.
- NGOs like Design 4 Democracy Coalition used CrowdTangle to help analyze the information ecosystems in places like Kosovo, Hong Kong, Moldova, and more in order to study the overall state of democracy around the world¹³.

And the list could go on. Truthfully, there was no shortage of use cases because of how critical social media has become to the political and civic discourse of the world and how essential that data is to the public.

However, ultimately, there was a limit to how far we could push transparency from within Facebook when it all came crashing down in May of 2021.

The Limits Of How Far Platforms Are Willing To Go On Their Own

It's not easy to work on transparency from inside a major social platform.

When an advocacy organization releases a high-profile report on how the company has been dropping the ball on climate misinformation¹⁴, and they cite your team's data, it's uncomfortable. When your data is misinterpreted to create a misleading narrative¹⁵ that is repeated for months on end in some of the most prominent news outlets in the country, it's uncomfortable. When there is a viral video about fake COVID cures¹⁶, and outside journalists only catch it because they are using your system, it's uncomfortable. When the White House uses your data¹⁷ to claim

⁹ https://secure.avaaz.org/campaign/en/climate_briefing_report/

¹⁰ <https://www.poynter.org/fact-checking/2020/the-ifcn-adds-crowdtangle-as-an-ally-in-the-fight-against-misinformation/>

¹¹ https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_.pdf

¹² <https://twitter.com/riovictoire/status/1446896304542650373>

¹³ <https://d4dcoalition.org/articles-list/using-crowdtangle-explore-democratic-contexts-around-world?page=1>

¹⁴ https://secure.avaaz.org/campaign/en/climate_briefing_report/

¹⁵ <https://www.businessinsider.com/facebook-right-wing-echo-chamber-data-executive-pushback-2021-7>

¹⁶ <https://www.theverge.com/2020/5/12/21254184/how-plandemic-went-viral-facebook-youtube>

¹⁷ <https://www.cnn.com/2021/07/16/white-house-says-facebook-needs-to-do-more-to-fight-vaccine-misinformation.html>

that your platform is failing to protect Americans around COVID and literally "killing people," it's deeply uncomfortable.

Those moments take a toll on your team. They also make it harder to get resources, they make it more difficult to launch new features or new data, and ultimately, they provide constant ammunition to executives who are skeptical about transparency at all.

On top of that, there are also organizational challenges that make it hard as well.

There are conflicting regulatory & legal requirements around the world that all are interpreted differently depending on which team or set of lawyers you talk to. There's the constant reality of regulatory pressure that encourages a "wait and see" approach instead of rewarding proactive efforts. There's a growing lack of trust between platforms and the media that covers them, which has meant increasingly less appetite to work together between the industries. There are some teams that believe in transparency but are never quite ready for it to be applied to their products. There's the fact that no matter how much transparency you provide, you're rarely going to get any public credit for it. And across the board, there is immense pressure to focus on short-term outcomes and constant, fierce competition for resources. And that's to name just a few.

But above all else, the single biggest challenge is that in the industry right now, you can simply get away without doing any transparency at all.

YouTube, TikTok, Telegram, and Snapchat represent some of the largest and most influential platforms in the United States, and they provide almost no functional transparency¹⁸ into their systems. And as a result, they avoid nearly all of the scrutiny and criticism that comes with it. That reality has industry-wide implications, and it frequently led to conversations inside Facebook about whether or not it was better to simply do nothing since you could easily get away with it.

Where To Go From Here

In October of 2021, as we approached the five-year mark of being at the company, there was finally an intense internal debate¹⁹ about the kind of transparency we provided and whether it was ultimately worth the public scrutiny and criticism that came with it. That debate eventually resulted in me leaving Meta²⁰ and my team of more than 50 people being reassigned to other projects or leaving the company altogether.

Today CrowdTangle is still available, but it's in maintenance mode. Meta has stopped onboarding new partners²¹, no new features or major updates have been released in over a

¹⁸<https://www.marketplace.org/shows/marketplace-tech/we-hardly-ever-talk-about-youtube-and-disinformation-not-anymore/>

¹⁹ <https://www.nytimes.com/2021/07/14/technology/facebook-data.html>

²⁰ <https://www.theverge.com/2021/10/6/22713109/facebook-crowdtangle-founder-brandon-silverman-leaves>

²¹ <https://www.cnn.com/2022/01/29/tech/facebook-meta-crowdtangle/index.html>

year, and a global partnerships team that used to run it no longer exists²². The tool is slowly dying, and one of Facebook's most significant commitments to transparency is very much up in the air.

Meanwhile, other major platforms, including ones that host large swaths of our civic and political information ecosystems, continue to do almost nothing to let the outside world look into their black boxes and face no real consequences. And all the while, as a country, we're only spending more and more time on social media as a country and continuing to see the powerful impact it has on us individually and societally.

While CrowdTangle has its limitations, I saw all the ways in which makes a difference. It helps monitor the most important discussions and debates of the day. It helps hold platforms accountable for living up to the commitments they've made to their users and the public. It helps make sure our new, digital information ecosystems are as open as possible instead of existing inside obscure black boxes. It helps advance our collective understanding about the role of social media in our lives and our democracies.

However, I think our experience is a bellwether; that the days of simply hoping that platforms will voluntarily share data are over. It's simply too easy for platforms to do nothing. I believe it's time to create legislation that sets some baselines for what we as a society expect and demand.

That's why in the last few months, I've been consulting with lawmakers around the world who are considering transparency legislation, including in Europe, where data sharing & transparency are major parts of the Digital Services Act which passed in late April, as well as other pieces of legislation being considered in the UK, Australia, New Zealand, and more. Here in the United States, the Platform Accountability and Transparency Act represents a similar piece of legislation and one that I think would be a powerful step in the right direction.

Ultimately, transparency is one of the most powerful levers we have to help make sure that social platforms live up to their promise of helping protect free & open societies. And we have an opportunity here in the United States to be a global leader in showing the world exactly how to do that.

How To Get It Right

There's no shortage of challenges to getting any legislation around transparency and data sharing right, including balancing data sharing with privacy concerns, trade secrets, surveillance issues, the First Amendment, and more. Those issues are real, complicated, and in some cases, they'll require tough tradeoffs.

But that's why we need the government's help in deciding what those tradeoffs should be. The government, not a set of private companies, should be adjudicating those questions, hearing from civil society and experts, and helping craft a set of rules & requirements that would apply to

²² <https://sfist.com/2021/07/14/facebook-is-dismantling-crowdtangle-because-it-showed-the-platform-to-be-a-right-wing-echo-chamber/>

the entire industry. In fact, I think in many cases, the industry would welcome the government's role in helping set those rules.

But it's also important to realize that any legislative solution to transparency shouldn't have a one-size-fits-all approach.

We need solutions like CrowdTangle that make privacy-safe data available in real-time that are easy to use and widely accessible to a broad swath of civil society, if not the public writ large.

But that's just one pillar of what any comprehensive legislation should require.

The truth is there's no perfect data set, no magic metric, or no single tool that accomplishes everything we need. The vast majority of the public interest issues we care about require a variety of different approaches to studying & understanding them. That's why any transparency requirement should come in several different shapes and sizes.

Any comprehensive approach to transparency should include requirements that fulfill as many of the following needs as possible:

- Datasets and tools like CrowdTangle that make it easy to monitor the most important and influential public accounts on a platform in real-time,
- Mechanisms for sharing privacy-sensitive data in safe & protected ways with highly vetted researchers,
- Ways to archive and share sensitive content that has been removed for violating specific community standards that are particularly important to the public interest,
- Transparency around all advertising on a platform, not just social and political ads,
- Legal & financial protection for people scraping in the public interest,
- Ways for professional auditors to study the design of algorithms for harmful or unintended outcomes,
- Sampled content of datasets that help provide a holistic view of the platform, and
- Reports that use industry-wide accounting practices & definitions around content moderation, hate speech, election protection, and other public interest areas.

We also need approaches that reflect an industry that is constantly evolving. Any set of transparency requirements should be able to adapt its provisions at the same speed that the industry, bad actors & ordinary user behaviors are all changing on a constant basis.

Conclusion

The most important thing in this discussion is that without moving forward with legislation, we will continue to be in the dark about the real impact of social media on our lives. We're going to continue jumping from one anecdotal data point to another, from one leaked document to another, from one urban myth to another, without ever establishing baseline, evidence-backed conclusions about what problems we should focus on. And that means we're going to risk

having an internet that weakens free societies instead of a building an internet that protects them.

When I think about social media and a lot of the public discourse about the role it plays in our lives, I'm reminded of the anecdote about the policeman who sees a drunk man searching for something under a streetlight and asks what the drunk man has lost. He says he lost his keys, and they both look under the streetlight together. After a few minutes, the policeman asks if he is sure he lost them here, and the man replies, no, that he lost them in the park. The policeman asks why he is searching here, and the man replies, "this is where the light is."

For too long, our public discussion about social media has been focused on the moments when we briefly found ourselves under a streetlight. Whether it was because of leaked documents, individual anecdotes, or moments where a small group of researchers & journalists were given a glimpse into the systems, those are each fleeting moments of a single streetlight lighting up a tiny part of our digital world for a brief moment in time. We need are transparency solutions that are sustainable, industry-wide and operating at a much larger scale. It's time to turn on the lights for good. It's time to pass legislation making it clear what we expect platforms to share and how to share it in safe and responsible ways. We've been wandering in the dark for too long.

