S. HRG. 117–840

BIG DATA, BIG QUESTIONS: IMPLICATIONS FOR COMPETITION AND CONSUMERS

HEARING

BEFORE THE

SUBCOMMITTEE ON COMPETITION POLICY, ANTITRUST AND CONSUMER RIGHTS

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 21, 2021

Serial No. J–117–35

Printed for the use of the Committee on the Judiciary

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

U.S. GOVERNMENT PUBLISHING OFFICE
54–862 WASHINGTON : 2024

COMMITTEE ON THE JUDICIARY

RICHARD J. DURBIN, Illinois, *Chair*

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

CHARLES E. GRASSLEY, Iowa, *Ranking Member*
LINDSEY O. GRAHAM, South Carolina
JOHN CORNYN, Texas
MICHAEL S. LEE, Utah
TED CRUZ, Texas
BEN SASSE, Nebraska
JOSH HAWLEY, Missouri
TOM COTTON, Arkansas
JOHN KENNEDY, Louisiana
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 COMPETITION POLICY, ANTITRUST AND CONSUMER RIGHTS

AMY KLOBUCHAR, Minnesota, *Chair*

PATRICK J. LEAHY, Vermont
RICHARD BLUMENTHAL, Connecticut
CORY A. BOOKER, New Jersey
JON OSSOFF, Georgia

MICHAEL S. LEE, Utah, *Ranking Member*
JOSH HAWLEY, Missouri
TOM COTTON, Arkansas
THOM TILLIS, North Carolina
MARSHA BLACKBURN, Tennessee

KEAGAN BUCHANAN, *Majority Staff Director*
WENDY BAIG, *Minority Staff Director*

C O N T E N T S

SEPTEMBER 21, 2021, 2:51 P.M.

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS

Page

ANSWERS

BIG DATA, BIG QUESTIONS: IMPLICATIONS FOR COMPETITION AND CONSUMERS

TUESDAY, SEPTEMBER 21, 2021

UNITED STATES SENATE
SUBCOMMITTEE ON COMPETITION, POLICY, ANTITRUST, AND CONSUMER RIGHTS,
COMMITTEE ON THE JUDICIARY
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:51 p.m., in Room 226, Dirksen Senate Office Building, Hon. Amy Klobuchar, Chair of the Subcommittee, presiding.

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

Also Present: Chair Durbin, Senators Padilla and Cruz.

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

Chair KLOBUCHAR. Okay. We've been joined by my friend and colleague, Senator Lee, so we're ready to begin the hearing. I call to order the hearing of the Subcommittee on Competition, Policy, Antitrust, and Consumer Rights on Big Data, Big Questions: Implications for Competition and Consumers.

Good afternoon, and before we begin, the Chair of the Committee can only be here for the first few minutes. It was very important to have him here and as we would give Senator Grassley the same due, we will—I asked Senator Durbin if he could say a few words before I begin.

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

Chair DURBIN. Thank you very much, Senator Klobuchar, and to our witnesses and my colleague Senator Lee for giving me this opportunity to say a few opening words about the scope and unrestricted nature of big data collection.

In 2018, we had an extraordinary hearing with the head of Facebook, Mr. Zuckerberg. He faced 42 Senators who had questions for him because of overlapping jurisdiction of the Committees. It was an ordeal that went on for some period of time. I was somewhere in the middle of the pack. The question I asked him was very basic. "Would you mind sharing with us the name of the hotel you stayed in last night?" After a kind of embarrassed and awkward pause, he said, "No." I said, "Well, would you mind sharing with us the emails that you've sent out in the last 24 hours and who you sent them to?" He said, "No." I said, "Really isn't that the

issue we're getting down to, privacy? Am I right to say there's a line I'm going to draw, and you can't cross it legally to invade my space and invade my privacy?"

In today's world, information is economic power. Companies are using it to make more money. I share the concerns of my colleagues that have enabled the collection of too much information by selected few giant companies. There could be benefits and efficiencies to big data, but there are cost and impact. These cost and impact affect everyone, including our children.

I introduced the Clean Slate for Kids Online Act because I was concerned with the amount of data collected and stored on our children and grandchildren. Every click a child makes on the internet leaves a trail of personal data that can last a lifetime.

Companies that market online products and apps geared toward children are accumulating massive amounts of personal data, and the kids never had the chance to even consider giving informed consent.

My bill would give every American enforceable legal right to demand that internet companies delete all personal information collected about a person when she was—he or she was under the age of 13. Kids deserve the right to request a clean slate once they've grown up and are old enough to appreciate the consequences of data collection. This bill gives them a basic privacy protection. It's one aspect of data collection that can be manipulated and impacted on consumers and competition.

Today's hearing is an important part of that effort to shine light on big data collectors.

I thank Senator Klobuchar and Senator Lee.

Chair KLOBUCHAR. Thank you very much, Chairman Durbin. I wanted to make clear that this hearing is one of a series of hearings that Senator Lee and I are conducting, our bipartisan review of America's competition issues. I thank my staff, as well as Senator Lee and his staff, for helping to plan the hearing.

Today we're going to be talking about how competition is affected and threatened by the use of big data. Big data is at the core of our modern economy, as Senator Durbin so well pointed out, powering targeted advertising and driving artificial intelligence to select what products and services we are shown online and increasingly offline as well.

In this hearing, we'll explore the companies that control the data, the state of competition and barriers to entry, and the effects of big data on consumers, their choices, and their privacy.

I'd like to be clear about what we mean when we say big data. Technology companies such as Google, Facebook, and Amazon collect an enormous amount of information, as Senator Durbin pointed out, about our daily activities in real time. They know what we buy, who our friends are, where we live, work and travel, and more.

In fact, their very business models, their very business models were set up around getting that information and then using it to profit. Through services such as Google's Gmail and Facebook's Instagram, though those services are offered to us for free, these companies and advertisers use the data they collect about us to sell to other companies. In the end, you can't get around the fact. We

are the product. We are the product that makes the companies money.

Big tech companies are not the only ones keeping tabs on all of us. Data brokers including Kinesso and its sister company, Acxiom, also buy, process, and sell massive amounts of personal information about consumers, and they've actually been doing it since before we even knew what the internet was. They collect information from the Department of Motor Vehicles, from public records, from our grocery store loyalty cards, and even from other data brokers.

Today they also buy our browsing histories, and guess how much money we make, and what religion we practice. This data has immense competitive value and the way that it is collected and used has important impacts on consumers.

I'll give you an example. The simple act of a consumer visiting a utility company's website to pay a monthly gas bill allowed dozens of companies to profit off of her, for the most part, without her knowledge.

Facebook and Google are likely to know about that consumer paying her bill even though they had nothing to do with the transaction. If the gas company runs advertisements on Facebook as many do, Facebook would have trackers embedded on the gas company's website. If the consumer, if she uses the world's most popular web browser, Chrome, Google would know what websites she visited.

Both companies collect and analyze this kind of information, building a detailed profile of the consumer and giving advertisers access to our online, for a price of course, but not something she gets paid.

At the same time, data brokers like Acxiom are buying and selling data from utility providers, so they also potentially know that she paid her gas bill, and they pair that information with her other purchasing habits, location data, financial information, family details, and their guesses about her race and gender. They sell this kind of information to governments, advertisers, healthcare companies, and others.

Just a few years ago, Acxiom had a partnership with Facebook to combine their data for advertisers and share the profits. At that time, Facebook would have supplied the consumer's online activities and Acxiom would have provided her offline activities, and advertisers could use them both to show her ads. Facebook ended that program in 2018, raising questions about whether massive technology companies now have so much data that they don't need to buy from data brokers.

In today's hearing, we will discuss how this kind of control over enormous data affects competition. While data-driven targeting can filter out things we don't want, show us products that might be of interest, and help some small businesses reach new customers, it also functions as a gatekeeper to important services and opportunities.

We talk a lot in this space, as Senator Durbin did, about the privacy concerns, and obviously, there's big concerns about that. I've been a longtime advocate for privacy legislation, Federal privacy legislation. I think its time has long come, and I know we are look-

ing at focusing some resources into these privacy issues in the bill that's currently being debated in the Senate.

We also have to look at another piece of this, and that is that there are real threats to fair competition from these massive data sets and the artificial intelligence inferences that these companies make based on them.

For example, after years of complaints and a Federal lawsuit, Facebook is reportedly still disproportionately showing job ads for mechanics to men and for pre-school nurses to women. That distorts labor markets, and it doesn't help us get to where we need to be to be able to recruit people for these jobs.

We also see the control that big data has serious implications for healthy competitive marketplaces. Data can be a barrier to entry. Unless you have a lot of it, you may not be able to reach consumers successfully. The big data allows you to target ads, to create algorithms that others who might want to be entering the market can't do if they don't also have the data. It can be another way that powerful internet gatekeepers maintain control of how small businesses reach customers and earn outsized profits from that control.

The impact of big data should also play an important role in merger analysis. As dominant digital platforms try to acquire other companies with massive troves of consumer data, the antitrust agencies must place greater emphasis on determining the competitive impact of obtaining even more data through mergers.

This is why I talk about that our laws have to be as sophisticated as the markets that we today operate in. We all want opportunities for new and innovative companies to emerge and for new markets to develop.

When big data inhibits competition by allowing those who have it to block access to markets for those who do not, we need to step in and fix it. This means enforcing our existing antitrust laws to their fullest extent to protect competition. It means updating our antitrust laws for the modern economy, just as we've done centuries past.

It's like every 50 years or so, we do a major update. The time has long passed for today's tech world.

My bill, Competition and Antitrust Law Enforcement and Reform Act, would do so by updating the legal standard to prohibit harmful mergers and anticompetitive conduct, shifting the burden to dominant companies to prove that their acquisitions and, most significantly here, their exclusionary conduct doesn't threaten competition.

We also have to make sure that our antitrust enforcers have the resources to do their jobs. They can't take on the biggest companies and some of the most complex conduct the world has ever seen with duct tape and band-aids.

Senator Grassley and I, with the support of this Committee, got our bill through to update the merger fees which will bring in over $100 million for both agencies. It has passed the Senate. We are waiting action in the House. We have every reason to believe we'll get it done.

There's more we can do not only in the reconciliation bill before us, but in the year-end budget to make sure these agencies have what they need.

We also need competition reform specifically targeted at tech. These are things like issues of interoperability. We've been talking about app stores recently. There's a major bill on that, bipartisan, that's been introduced, as well as bills targeting discriminatory conduct with tech companies.

As we explore paths forward, we see that the dynamics of data mining are already changing. In recent months, Apple rolled out an update that lets iPhone and iPad users decide whether they want to be tracked online by Facebook and other apps. That was a major good change. What happened? What do we know so far? Early reports indicate consumers have overwhelmingly opted out of being tracked. More than 75 percent, Senator Lee, decided not to be tracked on apps or their Apple devices when they were posed that simple straightforward question.

As we push for increased consumer privacy, we must make sure that monopolists don't fool us into handing over all control of our data to them at the expense of fair competition. We must both fight monopolies and protect consumer data. Guess what? We can do both things at once.

I don't want us to not realize this brave new world we are in, where having the data at all completely advantages certain companies who are the gatekeepers and makes it much more difficult to have a competitive market.

I will now turn it over to Ranking Member Lee. Thank you.

OPENING STATEMENT OF HON. MICHAEL S. LEE, A U.S. SENATOR FROM THE STATE OF UTAH

Senator LEE. Thank you, Chairwoman Klobuchar. I like the band-aids and duct tape analogy. I knew a guy named Fred Trent who used to say, "If you have a spool of baling wire, a roll of duct tape, and a pair of vice grips, you can fix anything."

Chair KLOBUCHAR. Okay.

Senator LEE. I'm sure he wasn't talking about antitrust laws. Yes.

Chair KLOBUCHAR. Maybe not this. Yes. Thank you.

Senator LEE. I think the title of today's hearing is an apt one, as big data does itself by its very nature present big questions, although the answers might not always be what we expect.

On the one hand, data is increasingly valuable and it's often essential to developing and improving technologies that'll power our economy through the rest of the 21st century. These technologies obviously have a bearing on consumer markets and retail markets, but they also make enormous contributions to national security and national defense and likely influence global strategic thinking in countless ways.

At the same time, as more and more data about us is collected, the risks of unauthorized disclosure increase considerably. The more valuable and the more useful our data becomes the more companies will do to obtain it, and the more we can start to expect more intrusions into our privacy.

Privacy, too, can be weaponized to entrench market incumbents and provide them with the convenient pretext for excluding competition and, in some cases, evading it altogether.

I see several key considerations going forward. The first is the value of our data. Viewing user data as a form of payment for online services is no longer just a theory. It's how the companies themselves, and how many antitrust enforcers, view the market. It's time for lawmakers and for the public to catch up, and we need to reframe our understanding and our expectations of supposedly free online services. To realize that they're not, in fact, free at all, but they come at the cost. A cost that's often opaque, unstable, and significantly greater than we may realize.

The second consideration, which flows naturally from the first, is the need to reinforce our ownership and our control over our data. When we recognize the value of the data that we provide for companies like Google and Facebook in exchange for their services and realize the massive imbalance in bargaining power the consumers have had—had up until this point, it should compel us to take greater care that our data is truly ours, that we have the ability to meaningfully consent to its use and to revoke that consent.

Each of these will help to promote competition in markets that rely heavily on data by forcing companies to compete for the quality of services offered in exchange for our data and for the right to continue using our data.

Speaking of data and product quality, it's often claimed that better data will mean better services. That depends entirely on how the data are put to use. Intrusions on our privacy are an obvious threat to quality, but so too are the more insidious threats like those uncovered recently by the Wall Street Journal about Facebook. It may be that the most pressing question when it comes to data access in aggregation is not whether it's entrenching monopolies, but whether it's leading big tech firms to act with flagrant disregard for the effects of their businesses on society at large.

Finally, we should be reticent to immediately embrace concerns that focus merely on the bigness of data access or aggregation. Data is not a finite resource. It's constantly being generated by innumerable sources, and no one company could likely ever control all data necessary to its or a competitor's business.

Moreover, punishing companies for obtaining the data sets necessary to achieve economies of scale and scope smacks of penalizing success, and it's not something we should be doing.

In the name of tearing down all barriers to entry, will we next demand that market incumbents share their trade secrets, their expertise, and their intellectual property with competitors?

All these questions and more should make for a deeply interesting and informative discussion, both at today's hearing and in the years to come. I look forward to it. Thank you, Madam Chairwoman.

Chair KLOBUCHAR. Thank you very much, Senator Lee. I'm going to introduce our witnesses now. Some are remote, some are here with us.

Steve Satterfield. Mr. Satterfield is a vice president on the Public Policy Team at Facebook. He leads a team responsible for developing and advocating for the company's positions on privacy and data related regulations. Prior to joining Facebook, he worked at Covington & Burling as a privacy lawyer.

Markham Erickson. Mr. Erickson leads Google's Centers of Excellence, a global team of subject matter experts focused on the application of law and policy with respect to technology and the internet. Prior to joining Google, Mr. Erickson was a partner at Steptoe & Johnson.

Sheila Colclasure. Ms. Colclasure is the global chief digital responsibility and public policy officer at IPG Kinesso. She is responsible for leading the global data policy and digital responsibility strategies at the company. She previously worked at the sister company, the data broker Acxiom as its global chief data ethics officer in public policy executive. She also served as staff assistant here in the United States Senate. I always like to add that when they do.

John Robb. Mr. Robb is an author and podcaster with The Global Guerrillas Report. He is alumnus of the United States Air Force Academy and Yale University. He previously served in uniform as a pilot and with the Special Forces. He is also the author of the book, "Brave New War."

Charlotte Slaiman has been with us in the past. Ms. Slaiman is the competition policy director at Public Knowledge, a nonprofit dedicated to promoting freedom of expression and open internet, and access to affordable communications. Prior to joining Public Knowledge, she served as an attorney with the FDC, and here in the Senate as a legislative aide.

We thank you, and if the witnesses could please stand and raise your right hand, including our remote witnesses.

[Witnesses are sworn in.]

Chair KLOBUCHAR. I will now recognize the witnesses for five minutes of testimony each, and why don't we begin with you, Mr. Satterfield. Thank you.

STATEMENT OF STEVE SATTERFIELD, VICE PRESIDENT OF PRIVACY AND PUBLIC POLICY, FACEBOOK, MENLO PARK, CALIFORNIA

Mr. SATTERFIELD. Thank you. Chairwoman Klobuchar, Ranking Member Lee, and Members of the Subcommittee, good afternoon, and thank you for the opportunity to be here today. My name is Steve Satterfield, and I'm vice president of privacy and public policy at Facebook, where I focus on developing and sharing the company's perspectives on data regulation globally.

I appreciate the Subcommittee's interest in the topics of today's hearing and the work that you all do to ensure the competitiveness of American markets and to shape data policy. I believe Facebook has an important perspective here given the substantial contributions we've made to the technology sector in the nearly 20 years since our founding.

We believe that many of the concerns expressed by Congress and other stakeholders with respect to privacy and content moderation can be addressed by appropriate legislation, and we stand ready to be a productive partner in those efforts.

As you know, our company is currently facing multiple lawsuits, including those brought by the Federal Trade Commission and a number of State Attorneys General, and that will limit what I'm

able to address today. I assure you we want to be helpful where we can, and I look forward to our discussion.

Like many services, Facebook helps people share, connect, communicate, or simply find entertaining content. Each day, millions of Americans use Facebook to connect with people and businesses, to share and view a wide range of content, to join communities of interest, and to set up fundraisers for good causes, among many other things.

All of these activities support our mission to give people the power to build community and bring the world closer together. The data helps make all of this possible.

At Facebook, we use and analyze data responsibly to provide personalized user experiences. We also use data to improve our products, to provide measurement, analytics, and other business services; to promote safety, integrity, and security; to communicate with people who use our services; and to research and innovate for social good, including by connecting and lifting up marginalized communities and addressing humanitarian crises.

Data also helps us show people better and more relevant ads, which keep Facebook free. It lets advertisers reach the right people, which benefits more than ten million businesses and non-profits. For the data people trust us with, we recognize that we have an important responsibility to protect it, and we work around the clock to help protect people's accounts, and we build security into every Facebook product.

We offer a number of tools that provide people transparency and control over the data we receive, and we've steadily made improvements to the privacy protections and controls we offer. We also have a variety of tools to help users understand the data Facebook has about them. We're always working to develop technologies that enhance the way people connect and communicate, and data is key to that work. We know that if we don't keep innovating and improving, we'll fall behind.

When Facebook started, we faced established competitors, including AOL and MySpace, with lots of user data that didn't protect them from competition. Success comes from creating products users value and enjoy, not from how much data you have.

As our CEO, Mark Zuckerberg has explained, we believe that strong and consistent competition is vital because it ensures the playing field is level for all. Facebook competes hard because we're up against other smart and innovative companies. We know that our future success is not guaranteed, especially in the global tech industry defined by rapid innovation and change.

Technological innovation has created an ever more competitive environment, and we invest heavily in our products and services to stay relevant, competitive, committing more than $18 billion to research and development last year. We're proud of our record and will continue to focus on building and updating our products to give people the best experiences possible.

Thank you and I look forward to your questions.

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

Chair KLOBUCHAR. Thank you very much, Mr. Satterfield. Next up, Markham Erickson of Google.

STATEMENT OF MARKHAM ERICKSON, VICE PRESIDENT OF GOVERNMENT AFFAIRS AND PUBLIC POLICY, GOOGLE, WASHINGTON, DC

Mr. ERICKSON. Chairwoman Klobuchar, Ranking Member Lee, and distinguished Members of the Subcommittee, thank you for the opportunity to appear before you today.

My name is Markham Erickson, and I'm a vice president of government affairs and public policy at Google, where I oversee a global team of subject matter experts focused on the application of law and policy to technology and the internet.

Data should be used to make consumer's lives better by improving the quality and diversity of products and services available, while protecting user's privacy and giving them control.

In my testimony, I will describe how Google uses and protects data, the safe data mobility empowers consumers and boosts competition, that data alone does not guarantee better products for consumers.

Data plays an important role in making Google products and services people use every day functional and helpful, and we are committed to treating that data responsibly and protecting privacy with strict protocols and innovative technologies. Google combines industry-leading technology with insights from data to develop products that help people find directions, build businesses, and search for information.

On an individual level, what data is collected and how it is used depends on how each person uses our services and how they manage their privacy controls. Data is one element of our ads business where it helps us connect people with relevant advertisements. Advertising is Google's main source of revenue, and it enables us to make many of our flagship—flagship products available for free to billions of people around the world.

The ads shown are often informed by a search query or page content, but they can also be based on a user's interest or their personal data, if their privacy settings permit. We do not sell our users' personal information to advertisers or to anyone. Our business relies on ensuring our user's trust, specifically in how we use and protect their data. We work to maintain that trust by offering industry-leading controls to manage privacy. Three billion users visit Google accounts every year, where they can review and change their privacy settings and delete data stored with their account.

We constantly innovate to improve privacy across our products and on our platforms. For example, Privacy Sandbox is a collaborative initiative that aims to build a more private and secure web, because many publishers and advertisers rely on online advertising to fund their websites and connect with consumers. We will continue to partner with the industry, civil society, and governments to get this balance right.

In addition to our work to advance privacy-preserving technology, we contribute data and expertise to the broader ecosystem. Data portability empowers consumers to choose services or online platforms based on quality and individual preference, not because they're locked in.

Since 2011, Google Takeout has enabled users to easily move their content to competing services with more than one billion gigabytes exported from Google products. Additionally, through our leadership in the data transfer project, Google makes it easier for other companies to provide tools that let users seamlessly move data between online services.

We are also proud of our contributions to the open-source community. Many of the larger successes in the machine learning ecosystem have come from data that is openly available on the web.

Senators, data by itself does not guarantee better and more and more successful products. Rather, it is the investment, innovation, and methods that matter, not just the amount of data that a company may have. Cutting edge technology or new ideas allow companies, new companies, to succeed, sometimes without any data at all. New entrants such as Zoom, Snapchat, Spotify, Pinterest, and many others, they've all become successful because they provide an innovative product, not because they have access to data from established companies.

Our focus is continually improving our products, and our greatest source of innovation comes from extensive research and development. Last year alone, we spent over $27.6 billion on research and development, which is nearly ten times what we spent in 2009.

At Google, we are committed to protecting data through privacy, security, and user control, and improving our products in a way that ensures more consumer choice and competition. We will continue to engage with policymakers and regulators, as well as other stakeholders, to support thoughtful regulation that encourages innovation and protects consumers. For example, we have long supported Federal privacy legislation in the United States, and we encourage to Congress to enact such legislation.

Thank you for the opportunity to discuss our work with you today, and I welcome your questions.

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

Chair KLOBUCHAR. Thank you very much Mr. Erickson. Next up, Ms. Colclasure.

STATEMENT OF SHEILA COLCLASURE, GLOBAL CHIEF DIGITAL RESPONSIBILITY AND PUBLIC POLICY OFFICER, IPG KINESSO, LITTLE ROCK, ARKANSAS

Ms. COLCLASURE. Chairwoman Klobuchar, Ranking Member Lee, Members of the Committee, good afternoon. Thank you for the opportunity to speak today.

I'd like to make several key points about the importance of fair and open data use, the intersection of data privacy laws and Federal competition practices, and their potential impact on today's connected marketplace.

First, responsible companies are ready for a comprehensive Federal data privacy law that is good for citizens and good for America. I work for Kinesso, a subsidiary of the Interpublic Group of companies or IPG, one of the largest and most data-driven advertising agency holding companies in the world. We strongly support a national privacy law.

IPG's business is built on four pillars of consumer trust: accountability, fairness, safety, and transparency. We work hard with our industry partners to instill these values throughout data-driven advertising.

Second, in today's economy, any privacy law, functionally, will be a competition law, whether a legislature intends it to be or not. America needs a future-fit national privacy law and appropriately applied antitrust policy.

In our connected marketplace, both of these have data availability, use, and control at their core. A Federal privacy law should be people-centered and ensure data is used to serve people. Limiting who can collect, control, and use data won't work. A privacy law that restricts who can collect data would give data control and, thus, market control to a few companies and unavoidably weaken competition. As we have seen in other jurisdictions, market power belongs to whoever controls the data.

A Federal privacy law should preserve data sharing for beneficial and innovative purposes, while making companies responsible and accountable for harmful uses. Similarly, competition policy should ensure that companies with better technology, better ideas, and innovation, but which may not have adequate data of their own, are not foreclosed from the marketplace. A company shouldn't have to create a first-party platform to compete.

Today's connected marketplace increasingly is dominated by companies who thrived thanks to ready access to consumer data. National laws that in effect limit data to just a few dominant players risks putting more power in those few players' hands. In our data-intense economy, overly restrictive data use and sharing laws preclude robust competition, vibrant innovation, and the possibility of the small company finding and competitively serving its audience.

We emphasize how essential data availability, open data flow, and fair uses of data are to innovation, competition, and a vibrant market of connected participants.

Federal privacy law and competition law should provide for responsible and accountable data sharing so that everyone can compete. We urge you to consider the effect of mergers on who controls the consumer data value change and, thus, on competition. An analysis of the growth of the major online platforms shows the role that acquisitions have played in the development of dominant data positions. To protect people, the fair use of their data, and support a robust, trustworthy, and competitive connected marketplace, Federal law should promote fundamental privacy rights for citizens and enable responsible accountable use and sharing of consumer data by commercial enterprise. This allows the market to continue to provide a wide array of benefits to people, including things like safer online payments, ready access to business and consumer credit, access to free content and platforms, and cost-effective and efficient advertising for all, especially small business and new market entrants.

We at IPG have built accountability and responsible data practices into everything we do. We believe that corporate America is ready to responsibly collect and share consumer data and be accountable for its actions in doing so. We encourage the Committee to protect the fair and open use of data as fundamental to competi-

tion. We urge the Committee to help develop a Federal privacy law that is future-fit for the digital age and protects consumers and enables a connected marketplace in which all participants can compete fairly, so long as they engage in safe and accountable data use and sharing.

I thank the Committee for its attention and look forward to your questions.

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

Chair KLOBUCHAR. Thank you very much. Next up, John Robb.

STATEMENT OF JOHN ROBB, AUTHOR, THE GLOBAL GUERRILLAS REPORT, ACTON, MASSACHUSETTS

Mr. ROBB. Thank you so much for the invitation. I'm a bit of an outlier here; I'm not a lawyer. Big data and the AI's that are articulated are clearly already valuable. They'll become more valuable over time as they're integrated into all of the products and services that will be sold in the next 20 or 30 years.

Unfortunately, there isn't a clear approach to how to deal with this big data in the marketplace. Currently, there is three major methods of actually dealing with data. We have it in China, where they have incorporated this big data into their national security and implemented a national security totalitarian state. You have in Europe, who's suppressing the aggregation of big data through privacy laws, basically turning it into something to be destroyed rather than embracing it. That'll affect their economic capabilities long term, reducing the capabilities to even produce high-quality products in the future, but, you know, it does award them better social stability. And then we have the U.S., which is still, you know, up in the air. We're still trying to decide what to do with it. If you use a framework on the economic model for the United States, the way we're treating data right now is very feudal. It's basically a feudal system where you have the corporations are acting as, you know, the lords and owners of the data, and they farm people for their data as they traverse their platforms. That's clearly not sustainable over the long term. You know, it will create, you know, wealth inequalities as big data and its AIs move toward the center of the economy. That, you know, that will also create the social instability.

The solution to that is the same solution we used to eradicate feudalism in the past, is that data ownership—is to give people ownership over their data so they can exercise ownership privileges associated with it and reap the benefits for having that ownership. That means taking data off the big platforms and putting it into a central repository, you know, that's controlled by the owner of the data, where it can be pooled with others and then resold or lent to organizations that will make use of it, build AIs that are useful in a variety of different ways.

It doesn't always have to be commercial. It could be open source efforts, it could be non-commercial university development, but putting the consumer, putting the individual in the driver's seat changes the whole equation. It could also be a source of royalties and revenues for that individual, driving their personal prosperity forward. It's a different way to approach it. It does destroy the data

directly through privacy, but it allows them to benefit from data as it moves forward.

There's also a strong tie between big data and these AIs to the national security component that's going to come into all of this tangentially. I don't think people would fully appreciate how much things have shifted over the last 20 years. All of the technologies that are needed to implement a national security data-driven surveillance state have leapt forward substantially, and that most of the shift has occurred within the context of the corporate development. We've seen a shift from what governments used to be only able to do to now corporations are only able to do it.

China has embraced that, and they're using those corporations to gather the data, create the tools, and control their society.

The problem here in the United States is that there aren't any natural limiting factors to prevent that from happening here. We don't have any protections against the overreach in the corporate realm. We don't have any—like we do against Government overreach. We don't have any free speech rights. We don't have any rights of access. We don't have the ability to resolve disconnection, because disconnection in the modern environment can radically reduce your ability to operate in the world.

We need a set of digital rights that we can exercise over—to protect us against any kind of overreach at the corporate side.

Thanks.

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

Chair KLOBUCHAR. Okay, very good. Thank you. Next up, Charlotte Slaiman, with Public Knowledge.

STATEMENT OF CHARLOTTE SLAIMAN, COMPETITION POLICY DIRECTOR, PUBLIC KNOWLEDGE, WASHINGTON, DC

Ms. SLAIMAN. Chairwoman Klobuchar, Ranking Member Lee, thank you so much for the opportunity to testify today on behalf of Public Knowledge, a nonprofit working in the public interest for over 20 years.

I'm Charlotte Slaiman, competition policy director at Public Knowledge. Gatekeeper power is at the root of big tech's competition problems. Experts, policymakers, and advocates the world over have identified gatekeeper power, sometimes bottleneck power, sometimes strategic market status, as the power that dominant digital platforms have over other businesses' ability to reach their customers.

Right now, big tech has the power, over us and our data, and we need to protect both users and a competitive market with new laws and rules to promote fair competition against them. Until we have a real choice to leave these platforms if we're not happy with them, they won't have the incentive to win us over, and we'll continue to miss out on disruptive innovations that challenge the status quo.

I want to take this opportunity to highlight important legislation that I think can help to address the underlying power dynamics that have led us here. Interoperability, data portability, and delegatability are the privacy-protective ways to neutralize the power that big data confers upon dominant digital platforms.

Right now, if I'm frustrated with how Facebook treats my data, I don't really have the option to leave, because my friends and family, the businesses, groups, and even schools I need to communicate with are on Facebook. Interoperability would allow competition to flourish by letting users communicate across platforms.

Look to the Access Act for a model of implementing interoperability to maximize competition and protect privacy. These platforms can abuse their gatekeeper power to freeze out would-be competitors from the market. One of the tools for that anticompetitive discrimination is big data. Gatekeeper platforms can put their own products first on the page, give them the best attention-grabbing design, and point users away from companies that pose a competitive threat. While this offends our basic notions of fairness, this behavior would be difficult to stop using our existing antitrust laws.

We need a nondiscrimination law to reliably stop it. I'm so glad to see news reports that Chairwoman Klobuchar is working on just such a bill here in the Senate. There's a strong model in the American Choice and Innovation Online Act from Chairman David Cicilline in the House.

Strict limitations on mergers by dominant digital platforms and giving our Federal antitrust enforcers the ability to sue to break up vertically integrated dominant digital platforms are also important parts of how we can address gatekeeper power. The Platform Competition and Opportunity Act and the Ending Platform Monopolies Act are strong examples of how these tools could work. These four bills were recently endorsed by a bipartisan group of 32 State attorneys general.

App stores and operating systems preference their own products when it comes to communication with the user and to data. The Open Apps Market Act zeros in on the gatekeeper role that app stores play.

Purposeful narrowing of our antitrust laws by the courts have left big business with a license to engage in a host of anticompetitive conduct. A myopic focus on price and other easily quantifiable effects leaves out important innovation and consumer choice harms that antitrust is supposed to address.

Chairwoman Klobuchar's Competition and Antitrust Law Enforcement Reform Act would help reign in the power of big data by updating the legal standards for blocking mergers and stopping exclusionary conduct. Competition is not a panacea for the challenges of big data. We also urgently need new privacy laws to protect users and a digital regulator to comprehensively address the policy questions surrounding digital platforms.

A comprehensive Federal privacy law can be procompetitive by creating a level playing field for dominant incumbents and new entrants alike.

For decades, Washington has taken the perspective that we need to let digital businesses run wild to see what great innovations they might come up with, but today, unscrupulous data practices and consolidated power have led us to a place that isn't anyone's dream of what the internet was supposed to be.

These largely unregulated platforms have been allowed to amass powerful gatekeeper roles where they need not fear competition or

Government intervention. For users to really have control, we need to have a real choice to leave these platforms. We need real competitors, and we need switching to be easy. To get those things, we need new laws and rules to promote fair competition on and against gatekeeper platforms like Google and Facebook.

Congress has already done the laudable work of introducing a series of bills to combat these harms. The best time to pass them was 10 years ago, but the second-best time is now.

Thank you.

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

Chair KLOBUCHAR. Okay, very good. All right. Why don't we start out, Mr. Satterfield, Mr. Erickson, Facebook, and Google both collect data about consumers to enable targeted advertising, which is the principal way I believe your companies make money. How important is consumer data to each of your companies? You can start Mr. Satterfield.

Mr. SATTERFIELD. Thank you, Chairwoman Klobuchar. The way that we look at it is success comes from building great products and not from how much data you have.

Chair KLOBUCHAR. Okay. Is—just if you could just straightforward answer the question, how important is consumer data to your company and your profit model?

Mr. SATTERFIELD. Data's important, you know, to connect people to relevant experiences. That includes showing them relevant ads, but again I'd say that you know, the success that we've had has come through building great experiences and not from the amount of data that we collect.

Chair KLOBUCHAR. Mr. Erickson, how do you answer that for Google?

Mr. ERICKSON. Thank you, Senator, for the question. At Google, we provide a means for people to find relevant information and helpful information on the internet, and to do that we have to understand what they're looking for. Anyone can use our products for free without providing or storing any personally identifiable information with us. We provide transparent mechanisms for users to understand how their data is being collected and how their data is being used, and meaningful tools to give consumers the ability to see the data that is stored in their account and to make choices like delete the data, or use one of our auto-delete tools to set up regular cadences where information, such as their search history or viewing history or location history if they've opted in to location history, can be regularly deleted.

We've also, as I mentioned in my testimony, since 2011, have created tools to give consumers the ability to take the data that they provided to us and move it to a competitor's site. We don't want users to work to engage with Google because they feel locked in because their data is with us. We want them to be able to go to the services and the technologies that suit their needs based on a competitive dynamic rather than any sense of lock-in.

Chair KLOBUCHAR. Okay. Why don't we go to you, Ms. Slaiman. I was just looking at some Twitter feed. Someone just reported that they were talking with a few friends on one of the sites, going back and forth online about being a female politician a while back, in-

cluding a TV make-up artist for some reason, and this person said they referred to me as inimitable online, and within an hour they got an online ad for Chanel Inimitable mascara, linking the TV make-up artist comment with their adjective. Is that possible? I don't know if this is true or not, but I'm just saying this is what's happened to me, and how important is the data to these companies? They've kind of gave round around about answers here. What does it mean for other platforms trying to compete if they don't have the data?

Ms. SLAIMAN. I think the data is very important. I appreciate what the other witnesses have said, that there is also a role played by their innovative engineers. I think that's absolutely right, but the data is important, and that's why we're concerned about whether it's being treated competitively or not. You know, I think the relevant ads are not always what is best for us. It's what's best for the platform, and sometimes that lines up with what's best for us, and sometimes it doesn't.

We need to make sure that we have protections for users and for the competitive marketplace when we're looking at that problem.

Chair KLOBUCHAR. Mr. Satterfield, along the same lines, last quarter Facebook publicly reported that its advertising revenue per users in the U.S. and Canada was $51.58. I want to ask you a few questions about that.

The comparable number for Europe was only $17.08. In Asia, it's $4.13. The rest of the world, you reported advertising revenue per user of about $3.00. Why is the value of a user in the U.S. worth so much more than the rest of the world, especially when we're comparing ourselves to comparable countries in Europe?

Mr. SATTERFIELD. Senator, I think there are a lot of factors that go into those average revenue per user numbers.

Chair KLOBUCHAR. Okay. I just—that's not really an answer though, man. That's the beginning of an answer, so.

Mr. SATTERFIELD. What we're doing is we're breaking down revenue per region according to the number of folks that we serve in those regions. That's what's reflected in the numbers that you're describing.

Chair KLOBUCHAR. Okay. Why don't we go to you, Mr. Robb? Do you think Facebook should pay all of its U.S. users $51.58 for Facebook's use of their data, which we now know, it's in their recent fiscal report? Maybe the individual profit centers, which is all of us, should actually get the money back?

Mr. ROBB. If you own the data, you would at least be able to compare offers and get paid for its usage. I don't think you'd get the full amount, obviously, but then——

Chair KLOBUCHAR. Right. Maybe there'd be a discount, but you could get a good chunk of it just like you do when you, you know, when you're a consumer and—they—you go and buy something or you sell something, is probably the better example.

Mr. ROBB. That's correct.

Chair KLOBUCHAR. Mr. Robb, when companies collect data about us and either sell it or use it to target us with ads, we aren't just the consumer or the user anymore. We really have to start thinking about this because I think when we get on these platforms, we, you know, can have fun, people do business, but they don't realize

every single second they're on there, they are creating profits, but they are not reaping the benefit.

We are, in fact, our data is a commodity, but consumers as I know it aren't getting enough in return, and I've discussed the idea of somehow putting a tax on the data for these companies to pay. You have written about paying people for their data.

In your opinion, what is the strongest argument for ensuring that the tech companies have to pay for the consumer data that they collect and use, and if Facebook and Google had to pay for using consumer data, how do you think their behavior would change?

Mr. ROBB. Okay. The most compelling argument is that it would change the perspective people have on data if they were in—if they had ownership rights over it. By unlocking it by, you know, through ownership, you don't just limit the data to what—that Facebook collects or Google collects to what they can do with it. You then open it up to what all of these other companies can actually do with it, and they can generate revenue. You know, people in control of their data, people who have ownership of their data, they will be more willing to give more and if they can set permissions in terms of how it's used, they'll feel comfortable with it. They'll feel like they're participating in the economy rather than being observers or being treated as resources. It's a complete face shift. It's not even comparable to what we have now.

Chair KLOBUCHAR. Okay. I thought it was just so interesting. I'll go back to you, Mr. Erickson, Mr. Satterfield, my last questions here. I just thought it was interesting, when Apple unleashed the power of allowing people to opt out, that 75 percent did that, because I think it's probably because they did it in a pretty straightforward way. Because I know I tried to do it sometimes, and then I'm on some site and I don't know if I've opted out, and it's really complicated for people, or they make me opt in to try to do something, and I can't figure it out, and you're just trying to order something online.

Mr. Erickson, you've spoken about putting consumers' privacy preference first and giving them the ability to change what is collected and used about them. I understand how you think that protects user privacy, but from a competition policy perspective, it seems like we look beyond what benefits an individual user. Even if millions of consumers give you permission to collect and use their data, shouldn't we be concerned about the competitive impact of your exclusive access to their data, which you use to compete with companies that don't have that data? Do you want to answer that, Mr. Erickson, first?

Mr. ERICKSON. Sure. Thank you, Senator, for the question. At Google, we do want to make sure that consumers first understand how their data is being collected and how their data is being used, and we do want to give them meaningful choice about their use of their data.

Unlike Facebook, the user can use Google services for free. They do not need to establish an account or provide any personally identifiable information to Google. We never sell personally identifiable information about our users, even when they do sign in. They can delete that information at any time.

Most users, when they're using online services, are providing similar information, if not the same information, to multiple online services, so in that regard, the data's really—the data's really nonrivalist from a competition standpoint. It's easily gotten by other companies that want to purchase data from, for instance, data brokers, or other entities, but I think the key here for us is to put users in a position where they have meaningful choices and meaningful control about the use of their particular data.

Chair KLOBUCHAR. Okay. Do you want to take a crack at that one, Mr. Satterfield, from Facebook's perspective?

Mr. SATTERFIELD. Yes. Thank you. Just to be clear, Facebook services are also free. To your question, Chairwoman Klobuchar, you know, the statistics are so interesting right now. The average user has something like 46 apps that they're using every month. There's more than 100 apps on the average person's phone. People are sharing more data in more places than they ever have been before. We think that there's a lot of data out there that's being used for innovative purposes, including to show people ads.

Chair KLOBUCHAR. Do you think they all know that they're sharing their data on all those apps?

Mr. SATTERFIELD. Senator, we hope so. We think transparency and controls are core values of ours, though we think that they should be core values of other companies as well.

Chair KLOBUCHAR. No, I just—if you could answer though, do you think that they know they're sharing that data? Do you think that they all know that?

Mr. SATTERFIELD. On Facebook, Madam Chairwoman, they do. I'm confident of that. There's core values of ours. We invest a lot in providing transparency and control. I think with respect to other companies, this is an area where Congress could intervene, make sure they do. Transparency and control could be core components of a Federal privacy legislation.

Chair KLOBUCHAR. Okay. I'm going to just ask just one follow-up because I really want a turn for Ms. Slaiman. Do you think that's true, that they all know this? Do you think we need—and by the way, the companies are now coming to us saying they want privacy legislation after opposing it, various iterations of it, after all the States have started to get into the act, which is kind of a pattern we've seen in other areas here, but do you want to respond to this quickly? Then I should let Senator Lee ask some questions.

Ms. SLAIMAN. Yes. I'm sure there are many users who do not know that they are sharing the data. I also think even if they know about the data that they're sharing, it's quite complicated to understand what that data can be used for. That data can be used to figure out additional information about you, so a user may be making a decision to share some data, not realizing what that data actually could tell a company about who they are and their preferences.

I also think I want to respond to the point that Mr. Erickson made about Google doesn't sell your data. I think it's important to keep in mind that Google has within them the capacity to fully exploit your data without ever selling it because they have the advertising system. Within this one large vertically integrated company, they can both collect the data and fully exploit it to advertise to

you, so the necessity for selling isn't there, and it can still be exploiting it just as effectively.

Chair KLOBUCHAR. Okay. Thank you very much. Senator Lee.

Senator LEE. Thank you. Mr. Satterfield, I'd like to start with you. I want to start by asking you about some recent reports about Facebook. The first is from Geoffrey Fowler at the Washington Post. He did a deep dive into Facebook's collection of user data, including revealing that Facebook's own financial modeling estimates that Facebook's estimates of its user data is worth an average of $164 per user per year. This would seem to confirm my own view and that of several State attorneys general, including my home State attorney general, Sean Reyes, in Utah, that Facebook isn't actually a free service, as you suggested a moment ago, but rather it's one that we pay for with our data. What's concerning is that there's so little transparency in the transaction, and you've sort of confirmed that now moments ago by saying that it is completely free. I am never told what my data is worth. You're not even acknowledging that it is worth anything or that there's any kind of a transaction involved here. What I get in return is always subject to change. You change systems by which posts are reviewed, what's prioritized, what deprioritized.

It's basic antitrust law that you look for symptoms. You look for signs. One pretty consistent sign of monopoly power involves the ability to set prices and control output. What could be a better example of that very thing than Facebook's ability to demand data from its users, as it does, without telling them its value or even acknowledging that it has a value at all, while providing a service whose quality, whose features, whose terms of service, in terms of use, are subject to change at any moment and they do frequently change at any moment?

Can you answer that question for me?

Mr. SATTERFIELD. Thank you, Senator. You know, respectfully, I think we see things differently. We don't see data as something that people give us in exchange for providing our services. We see data as something that we use to provide the service to them, to provide value to them.

Senator LEE. Okay, so you disagree with the assumption that when you're—when there's a service out there that purports to be free, you are the product. You are sort of what's being served. I mean, I get your point. Nobody's paying out of pocket with money. They're not paying in literal coins or virtual tokens to go on there, but you are in fact a for-profit business enterprise. You are in fact profitable, and you do that because there's something of value. I think we're quibbling here over sort of nonsensical distinctions between literal payment, which I didn't say, nor did I imply.

I guess I'd ask you to answer the question, accepting the premise that I think all the rest of us in this room and pretty much every other American would acknowledge exists, which is the premise that your service is—well, it purports to be free. It is in fact paid for in the sense that people contribute their time, they give their time, and with their time you acquire data. You're able to monetize that. With that understanding, I'm asking you, it is a basic principle of antitrust law that one sign of monopoly power is the ability to set prices and control output. With that premise, what's your re-

sponse to that? About the fact—I'm asking what better example could one find, once one accepts this premise, than that of Facebook's ability to demand data from its users without telling them the value of that data and without a service—when dealing with a service, whose quality and whose features and whose terms of service are subject to change at any moment and often do.

Mr. SATTERFIELD. Senator, you know, again, respectfully, that's just not how we think about data and how we use data to provide value to people.

Senator LEE. All right. All right, I get it. That's not how you think about it. It's clear to me you don't want to answer that, whatever. I was throwing you a bone there to try to allow you to engage in a dialog.

We'll move on to the next question. The Wall Street Journal released a series of bombshell reports last week on internal Facebook documents that revealed shocking, absolutely stunning lapses in Facebook's ability to protect Facebook's consumers, its users, from being harmed by using its platforms. This too looks like the behavior of a monopolist, a monopolist that's so sure that its customers have nowhere else to go that it displays a reckless disregard for quality assurance, for its own brand image, and even just being honest with its users about the obvious safety risks that it's subjecting its users to, particularly its teenage users.

In light of these reports doesn't it look to you like Facebook lacks competition?

Mr. SATTERFIELD. Senator, thank you. The Journal series that you're referencing raises, you know, really serious and important questions. I think it misses the mark in terms of what we're trying to do in the matters that it describes. These are——

Senator LEE. How does it miss the mark? How does it miss the mark any more than revelations years ago about tobacco companies concealing the dangers of tobacco? How is that missing the mark any more than the revelations about tobacco and what tobacco companies knew about what they were doing to their own users?

Mr. SATTERFIELD. Senator, I think what's being discussed in these articles are issues that we have identified ourselves and that we're attempting to work through as a company. This is research that we're doing ourselves in order to identify gaps and issues and to address them to make our platforms safer.

I think these are self-identified issues, and these are internal deliberations that are dedicated to one thing, which is making the platform a safer place for the people who use it.

Senator LEE. Ms. Slaiman, I'd like to turn to you. In your testimony, you advocate for updating the antitrust laws to tackle problems like big data. It seems to me that we have to first try to enforce the laws we have, which I think in most circumstances are more than up to the task, if in fact we will utilize them. If in fact, we will utilize the law and enforce the law. The reason we haven't used antitrust law to address many of the problems in big tech has everything to do with things that could be accomplished with the law. In other words, it's not just because the courts have said no. It's not because enforcers have taken these things repeatedly to the courts and the courts have smacked them down. That hasn't been

the case. It's rather been because our antitrust enforcers simply didn't bring the cases to begin with.

Look at the Obama administration. President Obama's antitrust enforcers let Google off the hook after a two-year monopolization investigation, ignoring—ignoring rather specific, rather conclusive staff recommendations to sue. They failed to stop Facebook from buying Instagram and failed to stop Facebook from buying WhatsApp, nascent competitors that they acquired at the time, and they failed to stop Google from buying its way to dominance of digital advertising.

Moreover, in the last year of the Trump administration alone, just the last year of that administration, the Trump administration, which finally filed cases against Google and against Facebook that the Obama administration had turned down, the FTC blocked 27 mergers. So far in 2021, the FTC, now supposedly run by antitrust hawks eager to protect competition, has filed just seven merger cases, one of which is the case against Facebook and five of which were filed in fact by the outgoing Trump administration.

Can't we agree that the problem with antitrust law isn't just the law but lacks antitrust enforcement?

Ms. SLAIMAN. Thank you, Ranking Member Lee. We absolutely need to improve antitrust enforcement. I believe it will be very important to improve the antitrust laws as well, but there have been lapses in enforcement.

I think there are some situations where the antitrust enforcers have correctly identified that the law wasn't there for them, but there absolutely are also cases that they missed that I wish they had brought. Improving antitrust enforcement is definitely an important part of this effort.

Senator LEE. Mr. Erickson and Mr. Satterfield, I want to ask both of you this question. The Wall Street Journal and the New York Times, they reported about a year ago that Google and Facebook had entered into an agreement to partner together with regard to digital advertising.

Setting aside the question of whether data can be a barrier to entry, shouldn't we at least be concerned when two companies with possibly the greatest access to user data secretly agree not to compete with each other for the primary way in which that data is to be used, which is digital advertising?

We'll start with you first, Mr. Erickson.

Mr. ERICKSON. Thank you, Ranking Member Lee. At the time of that agreement, we publicly announced Facebook's participation in our open bidding platform, as well as 25 other companies that are participating in that platform. We thought it would be useful to publishers and accretive to publishers where we'd have multiple ad networks competing for the publisher's inventory, and having large ad networks like Facebook benefits consumers. There's no truth to the allegation that these—our auction system is somehow rigged in Facebook's favor. If they provide the highest, bid they'll win. If they don't, they'll lose, but at the end of the day, those 25 companies which Facebook is one of them, creates more competition and more demand for the publisher's inventory.

Senator LEE. Okay. You're saying that just one of them, you're just two of those companies. You are in fact the two biggest, argu-

ably the two biggest companies with access to this much data. You don't see that there's any antitrust implication associated with this?

When two companies with possibly the greatest access to user data, agree not to compete with each other when it comes to digital advertising, you see no antitrust implications for that?

Mr. ERICKSON. Yes, Senator, respectfully, that's not the agreement. There is no prohibition for Facebook to provide their ad network and compete on other auction systems. Competing on Google's auction system with other ad networks creates actually more competition and more competitive dynamics, which ends up benefiting the publishers who are selling their inventory.

Senator LEE. Mr. Satterfield, my time's expired. Can you respond to that same question?

Mr. SATTERFIELD. Senator, I don't have anything to add to what Mr. Erickson said. You know, we compete hard. We compete fairly. We did so here as well.

Senator LEE. Oh, wow. I'm not surprised to hear that you don't think there's anything unseemly. We'll get back to that later. My time's expired. Thank you.

Chair KLOBUCHAR. Very, very good, Senator Lee. I was off in the other anteroom doing another hearing, and I can see you used your time well.

With that, we turn it over to Senator Blumenthal, and we've also been joined by Senator Hawley and Senator Cruz. Senator Blumenthal.

Senator BLUMENTHAL. Thanks, Madam Chair. I want to thank both you and our Ranking Member for holding this hearing. I hope it will be the beginning or maybe another step in an effort to forge a bipartisan effort on privacy law. I've been working with one of our colleagues, Senator Moran, on a draft for quite some time. We have come very close, and I am very hopeful that we'll continue to make progress because this issue of privacy is one of the central ones of our time.

There's no question as you, Madam Chair, have pointed out so well that data is the source of pay and power to these companies. It is not only a source of vast revenue; it is also the fulcrum of dominance and the ability to prevent others from entering the market, and the companies have learned how to do it very adroitly and have adapted to the challenges that have been put to them by the kinds of answers that we've seen today.

I want to return to those issues that my colleagues have raised so well. First, let me just ask a few questions about the Wall Street Journal investigative report that was published last week showing the heinously destructive impact of Instagram on teens. The simple fact of the matter is that Facebook has known for years that Instagram is directly involved in an increase in eating disorders, mental health issues, and suicidal thoughts, especially for teenage girls. Despite that horrifying risk, Facebook is now dead set on pushing Instagram to even younger children.

Far from being transparent about this danger, as Mr. Satterfield just attempted to represent, Facebook in fact has been blatantly deceptive and disingenuous about it.

Last month, on August 4th, Senator Blackburn and I wrote to Mark Zuckerberg and asked him specifically about this issue. We asked, and I am quoting, "Has Facebook's research ever found that its platforms and products can have a negative effect on children's and teens' mental health or well-being, such as increased suicidal thoughts, heightened anxiety, unhealthy usage patterns, negative self-image, or other indications of lower well-being?"

It wasn't a trick question. It preceded the published reports in the Journal. We had no idea about the whistleblower documents that were ultimately revealed. Facebook dodged the question. Quote, "We are not aware of a consensus among studies or experts about how much screen time is too much", end quote. We are not aware. Well, we all know now that that representation was simply untrue. Internal documents reported on by the Wall Street Journal demonstrate that Facebook has known for years that Instagram harms children and young people. For years, Facebook studies have found clear links between Instagram and mental health problems. It was common knowledge in the company, so the response was a clear attempt to mislead Congress and misinform parents. I ask that the Wall Street Journal report of September 14, by Georgia Wells, Jeff Horwitz, and Deepa Seetharaman be made a part of the record, Madam Chair.

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

Chair KLOBUCHAR. It will be. Thank you.

Senator BLUMENTHAL. Thank you. The comparison to big tobacco made by Senator Lee is entirely apt. I know something about big tobacco because I sued big tobacco and I remember the revelation of the documents that showed big tobacco not only knew but had done experiments proving that cigarettes cause cancer. They had denied it for years. They had the knowledge about the damage done to people who smoke.

My question to you, Mr. Satterfield, is, why did Facebook misrepresent its research on mental health and teens when it responded to me and Senator Blackburn?

Mr. SATTERFIELD. Senator, thank you. Respectfully, I don't agree with that characterization, but I do understand the frustration and concern that we're hearing about these reports. The safety and well-being of the teens on our platform is a top priority for the company. We're going to continue to make it a priority. This was important research. We're proud that we did it, and we're going to continue to, you know, study these really important issues.

Senator BLUMENTHAL. Why did you conceal it?

Mr. SATTERFIELD. Senator, we didn't make it public as we don't with a lot of the research we do because we think that that's an important way of encouraging free and frank discussion within the company about hard issues.

Senator BLUMENTHAL. Do you have more research that shows the destructive effect of your platform on teens?

Mr. SATTERFIELD. Senator, I'm not aware of any other research on teens. I don't work on these issues. I work on privacy and data.

Senator BLUMENTHAL. Are you not aware in the same way that the company responded that it was not aware when, in fact, it knew about the research?

Mr. SATTERFIELD. Senator, I apologize. I'm not familiar with the context of that letter or what went into the response. You know, what I can tell you is that we think it's important to be having a dialog with Congress on these issues, and we're prepared to work with you and your team going forward.

Senator BLUMENTHAL. Will you work with me and my team by appearing on September 30 at a hearing that we've invited you to do?

Mr. SATTERFIELD. Senator, I know our folks have been in touch with your staff, you know, to discuss that. It's something that I think we're discussing right now.

Senator BLUMENTHAL. We are discussing it right now. I'm asking you for a commitment that your company will send a high-ranking, qualified, and knowledgeable representative to that hearing on September 30. Senator Blackburn and I are, respectively, the Ranking Member and Chairman, but it includes Senator Klobuchar and Lee. They are Members, as well. We need to hear from someone who's capable of answering these questions, and it should be next week. Will you commit to have someone at that hearing?

Mr. SATTERFIELD. Senator, we're going to follow-up promptly on this. We know these are incredibly important issues, and we want to work with you and your staff going forward. We'll follow-up promptly.

Senator BLUMENTHAL. Mr. Satterfield, I just want to point out to you that your company, contrary to what you've just told this Committee, is continuing with this really unfortunate charade. Vice President Nick Clegg doubled down on the misleading statement, in fact, this weekend, when he said the research is, quote, "Still relatively nascent and evolving", end quote. According to one of these studies, Facebook found 13 percent of British users and six percent of American users traced a desire to kill themselves to Instagram. How is it not misleading to tell this Committee that the research is unclear if, according to your own research, tens of thousands of teens have suicidal thoughts directly because of Instagram? Don't you think you owe us an explanation next week?

Mr. SATTERFIELD. Senator, I appreciate the concerns. I do, and I do think that Nick was accurate in his op-ed. What I can tell you is that we can commit to working with you and your staff going forward on these issues.

Senator BLUMENTHAL. Has Facebook ever conducted research that found Instagram was more toxic to teens than another—other social media platform?

Mr. SATTERFIELD. Senator, I'm not aware of that but these, again, these aren't issues that I work on at the company. You know, we're happy to follow-up with you and your staff.

Senator BLUMENTHAL. Will you follow-up next—the September 30th by having someone at that hearing who can tell us the answer? By the way, the answer is that you have found Instagram is more toxic than Snap and TikTok. It's more of a Facebook problem. Your own research has shown it. I'd like somebody to come provide an answer, an explanation next September 30th.

Mr. SATTERFIELD. We're going to get back to you promptly, Senator. I can commit to that.

Senator BLUMENTHAL. I want to ask about another area but perhaps I should wait until I hope we'll have a second round?

Chair KLOBUCHAR. Yes, we will. We will.

Senator BLUMENTHAL. Thank you.

Chair KLOBUCHAR. Thank you. Thank you so much, Senator Blumenthal. Next up, Senator Hawley, then Senator Ossoff, and then you, Senator Cruz, if it works. Thank you.

Senator HAWLEY. Thank you, Madam Chair, and thank you, Senator Lee, also for holding this hearing. Thanks to the witnesses for being here. This is such an important topic. Mr. Satterfield, let me just pick up where Senator Blumenthal left off. Can I just ask you a fundamental question? Are teenagers safe on any of your platforms?

Mr. SATTERFIELD. Senator, we're working really hard to make that the case.

Senator HAWLEY. They're not now?

Mr. SATTERFIELD. Senator, we are investing a lot in safety and integrity across all of our platforms. We've invested billions of dollars.

Senator HAWLEY. Are you concerned, though, that teenagers are currently subject to all kinds of potential predators, the social effects—I mean, you're saying you hope that they'll be safe on the platforms? Are they not safe now?

Mr. SATTERFIELD. Senator, I think it's our responsibility to invest the resources that we need to make sure that these things don't happen. You know, that's why we're investing billions of dollars in protecting the integrity of our platforms.

Senator HAWLEY. By "these things" do you think things like this, let me read you a few quotes. "Thirty-two percent of teen girls said that when they felt bad about their bodies, Instagram made them feel worse." Quote, "We make body image issues worse for one in three girls", end quote.

New quote, "Teens blame Instagram for increases in the rate of anxiety and depression. This reaction was unprompted and consistent across all groups."

Or how about this? "Teens who struggle with mental health say that Instagram makes it worse."

Or how about this? "Social comparison is worse on Instagram."

Or about this? "Aspects of Instagram exacerbate each other to create a perfect storm when it comes to body issues, identity, depression, anxiety."

That doesn't sound like a very safe platform to me. Those, of course, are all from your own internal research. What do you have to say about that?

Mr. SATTERFIELD. Senator, again these aren't issues that I work on but I—we do have teams that are working across all of those issues, body image, well-being, and so forth. We're investing, you know, we're doing research like this so that we can identify gaps and address them. We're going to continue to do so.

Senator HAWLEY. Will you make the research public?

Mr. SATTERFIELD. Senator, again, you know generally the way that we approach research is that we keep it confidential to encourage free and frank discussion about it internally. It's—keeping it confidential actually enables us to——

Senator HAWLEY. Sounds like a no to me.

Mr. SATTERFIELD [continuing]. Ask hard questions about these really important issues.

Senator HAWLEY. I haven't been in the Senate that long, but this sounds like that's a no. Let me try again. You've already done the research. This research is completed. You've done it, you know the results, you know the data. You've actively misled Congress for years now. You've deliberately misled Senators as recently as just a month ago. Senator Blumenthal was just telling—putting on the record. You have the research. Will you make it public? Yes or no?

Mr. SATTERFIELD. Senator, I—respectfully, I'd strongly reject, you know, those characterizations. The issue of greater transparency around the research——

Senator HAWLEY. Let's try answering my question. Will you release the research? Yes or no?

Mr. SATTERFIELD. Senator, it's something we're looking into, how to provide greater transparency with appropriate context around the research——

Senator HAWLEY. Right. What would the appropriate context be, exactly? What's the context for 32 percent of teen girls saying that they feel worse when they use Instagram? Is there context that I'm missing there? What is it that parents need to know? What's the context, exactly? I'm intrigued by that statement.

Mr. SATTERFIELD. Senator, I mean, I think it's the broader view of what the potential impact of services could be on folks, and I think that the——

Senator HAWLEY. Oh, like maybe the things that Instagram does is positive that outweighs all of the terrible effects that it has on teen girls and others. Is that what you're talking about, your benefits? Let me ask you this. How much money does Instagram make for Facebook every year?

Mr. SATTERFIELD. Senator, I don't know the answer to that.

Senator HAWLEY. How much money do you make from teens being addicted to Instagram every year?

Mr. SATTERFIELD. Senator, I wouldn't agree with that characterization.

Senator HAWLEY. How much money do you make from your teen users every year?

Mr. SATTERFIELD. Senator, I don't know the answer to that question.

Senator HAWLEY. I bet it's a lot. I'll give it to you for the record. I think the—we all know what's really going on here. You won't release the research because this is a cash cow for you. You won't answer our questions because you make a gob of money on this. I mean, it's the whole reason Mark Zuckerberg wanted to get Instagram in the first place, right? I mean, back in 2012, Mark Zuckerberg wrote to his own chief financial officer that buying Instagram will give us time to integrate their dynamics before anybody else can get close to their scale. We know why Facebook bought Instagram. It was to get rid of a competitor, to gobble up all the data. Now they've done that. Now, it's making teenagers sick and destroying their mental health, but, you know, hey, it's lucrative. It's really—it's amazing. How about this?

Will you commit to suspending any efforts to develop the Instagram Kids product that would target children under the age of 13?

Mr. SATTERFIELD. Senator, we know that tweens are online, and, you know, we want them to have an experience that is a good one, that is a healthy one like we have with——

Senator HAWLEY. Like the one that teenage girls are having on Instagram right now, that kind of experience?

Mr. SATTERFIELD. Senator, respectfully, these are issues that we take incredibly seriously that we're investing in. You know, there is no more important priority than the safety and well-being of the people who use our products.

Senator HAWLEY. [Laughter] I really can't believe you're saying that. I mean, really, I've listened—I've listened to Facebook and these other big tech companies before these Committees for years, and I guess it's two years, although it feels like 20, and you always dissemble. You always mislead, but I can't believe that, given the research that you have conducted, that you can sit there and say that teens' health and security and safety's your top priority.

Clearly, it's not. You won't share any of the data. You're stonewalling every Member of this Committee. What about this? Will you at least commit to keeping behavioral advertising out of any product that a kid can access?

Mr. SATTERFIELD. Senator, we think that, you know, advertising is potentially very valuable. We have made changes with respect to teens under 18, limitations around the ability of advertisers to use our products to reach them.

Senator HAWLEY. Let's see. You won't reveal the research. You won't restrict your advertising. You won't pull back on plans to target children under the age of 13 with this platform, which you know is toxic for so many teenagers, especially female teenagers, and yet their health and well-being is your top priority. Do I—have I got that right? Did I miss any part?

Mr. SATTERFIELD. Senator, I'm not sure I said any of that. What I would say is, again, these are incredibly important issues to the company. We're committed to having a constructive dialog with Congress about them, and we're going to continue to invest heavily in them at the company.

Senator HAWLEY. I'm sure you'll invest heavily in it. I have absolutely no doubt about that. That I think is probably the truest statement you've made today. I have no doubt you will continue to pour money into Instagram as long as you can extract money from it and from the teenagers whom you are, quite frankly, exploiting.

Here's just a final question for you. Why should—why should you be able to advertise to teenagers at all? I mean, given all the dangers inherent in collecting their data, which is what you're doing on Instagram, why should you be able to advertise to teenagers? Why shouldn't we prohibit that?

Mr. SATTERFIELD. Senator, as you know advertising supports our service. We do think that additional protections for teenagers are appropriate. We put those in place. We're going to continue to look into ways to keep teenagers safe on our services while being able to support them with advertising.

Senator HAWLEY. Mr. Satterfield, the truth is you and I both know is that your product isn't safe. Your platforms aren't safe. They're dangerous. You know it, we know it. You stonewalled us. You've stonewalled the public. It's time for some accountability, and all I can say is accountability is coming.

Thank you, Madam Chair.

Chair KLOBUCHAR. Thank you very much, Senator Hawley. Before I turn it over to Senator Ossoff, I just want to—something when I was asking my questions that could lend some information to you here.

Facebook publicly reported that last quarter its revenue, advertising revenue per user, which I presume includes teens in the U.S. and Canada, was $51.58 per user. I guess just to follow-up, Mr. Satterfield, do you have the breakdown for teens versus the rest that we could get, maybe not today, but later?

Mr. SATTERFIELD. Senator, the only breakdown I'm aware of is the one you referenced, which is the average revenue per user.

Chair KLOBUCHAR. Does that include Instagram? Is it company-wide?

Mr. SATTERFIELD. Senator, I believe it's company-wide.

Chair KLOBUCHAR. Okay. All right. Senator Hawley compared it to some of the other countries which were a lot less than our country, so we'll have to be looking into that. How much revenue they make with that?

I'll turn it over to Senator Ossoff.

Senator OSSOFF. Thank you so much, Madam Chair. The first question please for you, Ms. Colclasure, does Acxiom or any other IPG company provide services to entities outside of the United States based upon or linked to data about U.S. persons?

Ms. COLCLASURE. Thank you, Senator, for your question. Of course, I'm at Kinesso and formerly at Acxiom, and a part of the IPG family. Acxiom data, we at Acxiom and at Kinesso both, we do have clients that are multinationals, and we have clients that operate in other markets around the world, and part of the services we provide are data-enabled services, marketing, and advertising services, so, yes.

Senator OSSOFF. Thank you. Do Kinesso, Acxiom, or other IPG companies provide data-connected services or services based on or related to data about U.S. persons to Federal agencies, State or local law enforcement, or any other public sector actors in the United States?

Ms. COLCLASURE. Of course, again, I'm speaking about Acxiom. Acxiom does have, and shortly to be retired, an identity authentication product, which is made up of regulated data and provided for regulated service and that is—we call that our risk product suite, and it solves things like know-your-customer obligations that financial services have—that we're actually exiting that business shortly and concentrating on marketing and advertising.

Senator OSSOFF. Is that the only product or service that you sell to any public sector entity in the United States?

Ms. COLCLASURE. We do other things like marketing and advertising data-enabled services. Like we supported an Ad Council advertising campaign to help get information out to help with the pandemic. Another example I can think of is we helped the Amer-

ican Red Cross when the Hurricane Katrina hit New Orleans several years ago. We helped get data to them for some marketing communications to go out and find audiences so they could learn about help and services from the American Red Cross.

We have a few other campaigns like that that I am aware of. Does that help?

Senator OSSOFF. Thank you, Ms. Colclasure. Do many IPG entities provide any services or have any financial relationships, direct or indirect, with any agencies or clients at the Department of Defense, in the intelligence community, or in Federal, State, or local law enforcement?

Ms. COLCLASURE. It is not an area of concentration, and I don't know the answer right off. I feel like I would——

Senator OSSOFF. Is that for the record?

Ms. COLCLASURE. Yes. I do not know the answer right off, but I promise I will go and research it and get you an answer so that I can be certain. Of course, there may be confidentiality issues that I'll have to navigate if we do have those sorts of contracts. I'm glad to go research and get you an answer.

Senator OSSOFF. Just to be clear, Ms. Colclasure, you are not personally aware and have never heard of any financial relationship between an IPG entity and the Department of Defense, the U.S. Intelligence Community, or any Federal, State, or local law enforcement entity?

Ms. COLCLASURE. I do know that Acxiom—of course, I'm not at Acxiom now, and Acxiom historically has had some relationships with some of that community, but I do not have the knowledge to share at this—but I'll research it for you.

Senator OSSOFF. What are you aware of? What do you recall?

Ms. COLCLASURE. We do have some—we did, again I'm not in command of the knowledge because I'm not at Acxiom now, but there are some Governmental agencies that we have worked with, most of it, like the Veterans Administration, was advertising and trying to do outreach to their veterans' community, so rather than fish around, if you might allow me, Senator, I'll go and research and get you an exactly right answer, if that would be OK?

Senator OSSOFF. Thank you. Do any IPG entities have direct or indirect financial relationships or provide any services or products to any foreign governmental entities?

Ms. COLCLASURE. Not to my knowledge.

Senator OSSOFF. Will you please double-check, for the record?

Ms. COLCLASURE. I certainly will. Certainly.

Senator OSSOFF. Thank you. How does Acxiom or how do other IPG entities engaged in their activities obtain device identifiers, such as IMEI or IMSI numbers?

Ms. COLCLASURE. At Acxiom and at Kinesso, of course, we operate in the digital advertising and marketing space, and we run a unified ethical framework as the basis for our data governance program. When we either source data, we undergo a due diligence process. I always like to say not all data's the same, and not all data uses are the same. Some of the data, like device IDs, that is a connecting piece of data that we use to enable and activate digital advertising campaigns on behalf of our clients. It may be that it flows in from one of our connected partner ecosystem providers,

like an advertising network or a publisher, and we sit in the middle as a connector. That is typically how the data flows.

Does that help answer?

Senator OSSOFF. Do you place any limitations? Does Acxiom or any IPG entity place any limitations on the form, category, type, of entities to whom you'll sell services?

Ms. COLCLASURE. Absolutely, Senator. Thank you for that question. We do. As I mentioned, we use what's called a unified ethical frame for our data governance program. We practice an accountability-based, data-governance program.

Senator OSSOFF. Which plans—forgive me, but my time is limited. Which types of entity specifically will you not license data to or provide services to?

Ms. COLCLASURE. We—they have to be a legitimate commercial enterprise. We don't provide data to individuals or data-enabled services to individuals. It is to commercial entities for a legitimate ethical purpose. We judge the data use in context via our privacy impact assessment process. We check it off against legal requirements, regulatory requirements, coregulatory requirements. We do a harm detection and prevention test, and then very important to all of us, we do a fairness test. I mentioned in my opening remarks that we're people-centered, and that is we design from people outwards, from the engineering layer outward.

Senator OSSOFF. Ma'am, my time is limited. I appreciate the elaboration of that policy. Let me ask you this question? Does any IPG entity or has any IPG entity provided any service or sold any product to private investigators?

Ms. COLCLASURE. No. A very long time ago there was one business that Acxiom owned that we divested that did serve PIs, but that might have been 10 or 15 years ago. The answer's no, today.

Senator OSSOFF. Which firm was that?

Ms. COLCLASURE. It was—it was Acxiom-owned. We had acquired an entity. We operated it for a few years, and then we sold it, and I apologize, I cannot recall the name right now.

Senator OSSOFF. Thank you, ma'am. Madam Chair, I may return for a second round if we have the opportunity. I yield.

Chair KLOBUCHAR. Excellent. Senator Blackburn.

Senator BLACKBURN. Thank you, Madam Chairman. Ms. Slaiman, let me come to you first. I know that you're aware that Senators Blumenthal, Klobuchar, and I filed the Open Market App Store Bill so that we could address Google and Apple and their stranglehold on that app market. Very quickly, how do Apple and Google's data practices factor into this app store and how they limit the use there, and do they incentivize the app store developers to continue the monopoly over—over this market that they have?

How are they manipulating that marketplace, very quickly?

Ms. SLAIMAN. Thank you so much, Senator Blackburn. We were so glad to see the introduction of the Open App Markets Act. I think that's going to be really important, not just for big data but for gatekeeper power writ large when it comes to app stores.

In particular, with regard to big data, I think the app stores and the operating systems have this privileged position where they can treat users, decisions about their data, differently, based on wheth-

er the app is owned by the app store company or the operating system company, or whether it's a competitor.

One thing that's really important is to make sure that those are being treated the same so that we have a level playing field for competition.

Senator BLACKBURN. I think that's important and that privileged position that they exercise is important to note. You've mentioned the gatekeeper property and how that would apply to other applications, whether it is publishers and other forms of content development. I think that this is an important bill that we get passed in on the record.

Very quickly on filter bubbles, and I know you've mentioned that—how do you address—how do you think we could address the filter bubbles and the platforms' secret algorithms, if you will, that really, kind of manipulate that consumer experience online?

Ms. SLAIMAN. One of the ways that big data is used is to decide what products to show the users. The platforms, again, are in this gatekeeper role where they're making those decisions. A lot of times that's based on an algorithm that is fed by data that they're collecting from users.

Those decisions about which products to show to users, which services to offer to users, those are decisions that the platform gets to make, and that's limiting the options that a user sees.

Senator BLACKBURN. Yes. I think that the Open Apps Market Act gives us that footing, as I said, that gatekeeper role to begin to address that so that the consumer, online consumer, has a more private and a more genuine experience, and we're looking forward to getting that bill passed. Thank you for those comments on that, because I agree with you. I think the implications we're going to see are writ large in the industry.

Mr. Satterfield, if I may come to you for just a moment. As you're aware, Senator Blumenthal and I have kind of been doing a deep dive on what you're doing with this data that you're collecting on teenagers. From working with whistleblower and from the data that we've seen, basically reams of data at this point, we are concerned about this amount of data that you are keeping on teens. Basically, what you're doing is building a virtual presence, a virtual you, of these teenagers. Do you think that is a violation of the Children's Online Privacy Act, the fact that you're tracking and following and building these files on these children?

Mr. SATTERFIELD. Senator, no. We're complying with the law. We do think it's really important to provide protections around teens' experiences on our services. These are things that we've been investing in. We've been consulting with third-party experts so that we do this thoughtfully and——

Senator BLACKBURN. Okay. Who are the third-party experts that you're consulting with? Because when we talk to teachers, to parents, to pediatricians, to psychologists, and when we look at the data that you have collected from teens and the changes that they have recommended that you make to your platform, it's like you're turning a blind eye to that because you're chasing a dollar. Why don't you bring some clarity to bear on that?

Mr. SATTERFIELD. Senator, this isn't something that I work on at the company. I'm happy to get back to you with more on the experts, and I'd say that——

Senator BLACKBURN. You know, if you're the VP——

Senator LEE. Still going.

Senator BLACKBURN [continuing]. On privacy and public policy, one would think that you probably were in meetings and that you would have a stakeholder position in what your company chooses to do on that issue. Are you not involved in these discussions of privacy and how to protect this data, and thereby how to protect the virtual you of these children and teens that are using your platform?

Mr. SATTERFIELD. Senator, yes, of course. I was talking about, you know, safety experts, experts on well-being and such. Yes, of course, I'm involved in privacy issues, including privacy issues that affect the teens on our platform.

Senator BLACKBURN. Do you have any plans in the works to use the data that you have collected, the data that teens gave you, the information they gave you when they participated in your mental health survey? Are you going to use that to put protections in place for these teens on your site? Yes or no?

Mr. SATTERFIELD. Senator, all of the research that we do, you know, informs the decision-making in the company. It's certainly something that we'll take into account as we're——

Senator BLACKBURN. The decision-making that you are exercising shows that you're making decisions that allow you to be more profitable, not that you're making decisions that are based on the welfare of that child. Why do you collect so much data on your users if you do not use it to improve the user experience? You're not using it to protect children or to improve the user experience, so for the record, why don't you tell us what you're using this data for?

Mr. SATTERFIELD. Senator, we are using the data that we collect when people use our services to improve their experience. That's our——

Senator BLACKBURN. Why would teens that took your mental health survey say—why would older teens say, "We're advising our younger siblings not to use Instagram, not to be a part of this online community"? Because they feel like you're not following what they're asking you to do. What are you using the data for? Are you using it for micro-targeting, to go in and target advertising? Are you using it to feed them—to push them further down paths if they click on one something then you keep feeding them more of that? Why don't you, for the record, tell us what you're using this data for? You've got reams of it.

Mr. SATTERFIELD. Senator, when it comes to the data that we collect when people use our services, you know, we do a couple of things. We use that data to provide the service. We use it to improve the service, to provide enhanced experiences, as you were saying.

Senator BLACKBURN. Tell me what improvements you have made that would keep teens healthier and safer. Give me three examples of things you've done that would keep teens healthier and safer as they use your platform.

Mr. SATTERFIELD. Senator, with respect to Instagram, we have made changes to the ways in which adults can contact potentially younger users. We've made changes to the way in which people can comment, and we've made changes that are designed to address potential bullying and harassment. In comments, we've made resources available on well-being and body image issues. We've made a number of investments over the years that address these kinds of issues.

Senator BLACKBURN. Do you nibble around the edges, or are you aggressive? Are you going to stop allowing human traffickers, sex traffickers, drug traffickers, to use your platform, whether it's in the U.S. or other countries? Is that the kind of improvement that you're making?

Mr. SATTERFIELD. Senator, respectfully, absolutely not. There's no place on Facebook for——

Senator BLACKBURN. It happens.

Mr. SATTERFIELD [continuing]. Activities like that.

Senator BLACKBURN. It happens. There's a Mexican drug cartel that's been on your platform. You didn't take them off.

Mr. SATTERFIELD. Senator, that organization was designated and banned on our platform, if what you're referring to is the organization from the Wall Street Journal article.

Senator BLACKBURN. You know, I have to tell you—and I have grandchildren, I have two grandsons and a granddaughter. My grandsons are 12 and 13, and my granddaughter is a year old. I tell my grandsons all the time that they cannot trust you all with their information. I think what you have done to a lot of these children is inexcusable. I think the fact that you collect this data, you monetize that data, you benefit from that data, and then knowing you have this data, don't you think parents would have liked to have known that this was taking place on your site? I do. I think it is unfortunate that you all have hesitated to answer the questions that Senator Blumenthal and I have. We do look forward to having a representative from your company come next week and answer the questions that we have in our hearing. Madam Chairman, we look forward to hearing more from Google and Apple about the Open Market Apps Bill. With that, I will yield back my time.

Chair KLOBUCHAR. Thank you very much, Senator Blackburn. Second round, Senator Blumenthal.

Senator BLUMENTHAL. Let me just say, Mr. Satterfield, if you fail to have someone here on September 30th, there can be only one reason, that you're continuing the concealment. Let me just be very blunt. You've been sent here to defend the indefensible, but at some point, Mr. Zuckerberg should get the message, "Houston, we have a problem." Better to be here on September 30, than continue to evade responsibility. I thank my colleague Senator Blackburn for putting it so succinctly and so eloquently.

I just want to point out that behind the numbers and the perhaps seemingly abstract questions there are real human beings, young women and men who are deeply hurt by these images, the focus on body images, on self-worth that comes along with those images. In one study of teens in the U.S. and the UK, according to the Journal article, Facebook found that more than 40 percent

of Instagram users who reported feeling unattractive, said the feeling began on the app, and about a quarter of the teens who reported feeling not good enough said the feeling started there, and many felt in quotes, "addicted" to the app and felt that they were deprived of self-control.

Again, the analogy to big tobacco is undeniable. It's an analogy, not an exact comparison, but the exploitation of that kind of attraction, even addiction, I think is reprehensible. I really do hope that you understand that there is a certainty here, which is accountability is coming, as Senator Blackburn has said and Senator Hawley put it exactly. Accountability is coming, and it will be bipartisan.

I want to shift to the issue that Senator Blackburn also raised, our bipartisan bill, the Open App Markets Act would set robust rules to promote competition and strengthen consumer protection. I am proud that this bill is bipartisan. I want to thank my colleague Senator Klobuchar for her leading role in this area and she is a co-sponsor of the bill. It's received wide support, as was mentioned earlier, from consumer groups, antitrust experts, and app developers. Ms. Slaiman, I especially appreciate your reference to it, and the support that Public Knowledge has provided for the bill.

Two companies, Google and Apple, have gatekeeper control of the dominant app stores that allow them to dictate the terms for everyone. Their duopoly allows them to set the terms and they do. If app developers don't like the terms, there is nowhere for them to go. That is what we call a broken market.

Not even Facebook is immune to Google and Apple's gatekeeper control, big as Facebook is, powerful as it is, it's not immune. Apple has blocked the Facebook Gaming app from the app store at least five times, and it has prohibited other cloud gaming services from becoming available on the app store. Apple has also forced Facebook to remove a notice informing consumers about the so-called Apple tax, that is the infamous 30 percent rent fee that they extract from digital goods and services. The little guy is as much a victim as the big guys like Facebook.

The Open Markets—Open App Markets Act would protect developers' ability to offer competitive prices, tell consumers about lower prices, and give consumers the right to make their own decisions about the apps they install. That's what's called competition, and a free market, or at least freer than it is now, and it would mean that Facebook and others don't have to pass the Apple tax on to consumers and small businesses.

It would mean that iPhone users could sideload Facebook Gaming directly on to their phones if Apple continues to block the app. These are basically pro-consumer and pro-competition rules.

Mr. Satterfield, would Facebook support Congress setting fair, clear, enforceable rules on app stores that would prevent Apple and Google from using their gatekeeper power to extract excessive rents and block competition like what happened to you and your app, Facebook Gaming?

Mr. SATTERFIELD. Senator, thank you. Our team is looking at the bill, and we're providing feedback through the, you know, the normal channels. You know, we're continuing to work with you and the other co-sponsors and providing that feedback.

Senator BLUMENTHAL. What are the normal channels?

Mr. SATTERFIELD. We're communicating with your staff and others.

Senator BLUMENTHAL. Okay. Let me point out, in case it isn't obvious, and I think it is, that Facebook really should support these kinds of rules if it is in favor of competition and open markets and not just for you, but for others.

Mr. Erickson, Apple has claimed that if we allow consumers to make their own decisions, all sorts of really horrible or terrible things are going to happen. Unlike Apple, Google has allowed sideloading and better developing access on Android from the very start. Given Apple's alarming claims, would you characterize everyone's Apple phone as insecure or vulnerable to cybersecurity risk, because that's what Apple says will happen if we eliminate the Apple tax of 30 percent?

Mr. ERICKSON. Senator, thank you for your question. If I may step back for a minute, we share the values that you and Senator Blackburn have that consumers should be able to choose the lawful applications, to download those, and that there should be competition in this marketplace. We're taking a look at your legislation as well, and we'll be happy to engage with you going forward.

The Android ecosystem, no, we do believe we provide a very safe and secure ecosystem for our app developers to reach a global audience of billions of users in 190 countries, and that's not undermined by allowing consumers to be able to download applications outside of the app store or to sideload those applications.

Senator BLUMENTHAL. You do believe Android is secure?

Mr. ERICKSON. Senator, yes.

Senator BLUMENTHAL. Let me just close this round of questioning, because I know my colleagues may have other questions. I cannot help but make this observation about the action just over the last weekend by Google and Apple, at the behest of Vladimir Putin, to censor their apps. In fact, censor apps that were used to organize democratic protests in Russia. Apple has taken down thousands of apps from its app store at China's request. Almost a third of them relate to human rights, and it includes Hong Kong protests and LGTBQ rights.

You know, in a tweet I analogized what's going on here to Neville Chamberlain and the attempt to appease Germany. I view it as very much the same kind of appeasement of Vladimir Putin and the Communist Party in China. I think it was Winston Churchill who said about Neville Chamberlain that he had to choose between dishonor and war. He chose dishonor and he got war. In fact, he got both.

At the end of the day, you're not going to appease these totalitarian dictators. Not even Apple or Google or any of the big tech companies are going to win by appeasement when it comes to human rights. I think that it's pandering. It's craven pandering, and it undermines our national interest, and I yield the floor, Madam Chair.

Chair KLOBUCHAR. Thank you very much, Senator Blumenthal. Senator Lee is next.

Senator LEE. Thank you very much. My next question is for Mr. Robb. Mr. Robb, what are the ramifications of our personal data having become the method of payment for so many online services?

Mr. ROBB. It's a loss of control, loss of income, and, you know, we're looking at the snapshot right now of the tech industry, and we're looking at—we're focusing in on marketing and the big players that exist today, but this is going to evolve. You know, I've been in the tech industry for decades, and I started on the internet 25 years ago, and that was well before Facebook and Google even existed.

The same thing's going to happen in the next 20-30 years, is that this data is going to persist, and we need to give individuals control of that data so they can learn how to exercise their control, set permissions on how it's used, and make money on commercial apps that actually use it to build products and services.

You know, changing the dynamic here——

Senator LEE. What if anything can we do to reassert our ownership and our control over our own data?

Mr. ROBB. I think the key way to do that is to get the data off of the platforms that are aggregating it, and then putting it into a central repository that's managed by the individual, and if they do that, they're in control. They're the focal point where actually combining that data and who's using it, rather than having it sold by third parties to third parties or—and combined in ways that they don't have any jurisdiction over.

By putting the, you know, the individual at the center of the equation, you know, it makes life more complicated, but it's an essential thing for us to move forward and be able to do this successfully long-term. Otherwise, we're going to be caught in this, you know, privacy trap. I mean, privacy's fine, but it really is just destruction of data and limitations on—rather than actually solving the problem at root.

Senator LEE. Are third-party brokers like Acxiom an obstacle or are they an aid to consumers trying to regain control of their data?

Mr. ROBB. The fact that they're combining data from multiple sources, they're actually acting in opposition to what individuals should—should be able to do. If you have the individual at the center of the equation, you don't need an Acxiom. We don't need a data broker. I mean, they can cut deals directly with them. They might even be managing the data repository. You know, it seems like—you know, we don't have a data repository now, and it seems, you know, fanciful to even think in terms of that, but I mean, we can build it. I mean, we can set the standards for how that would operate. We can lay out those standards and have companies actually compete to deliver on those standards, just like we built the web, just like we built so much of what we have in terms of web architecture.

You know, data aggregators can do business with individuals, but they can't be a substitute for them.

Senator LEE. Mr. Erickson, I'd like to turn to you next. In the last year, Google announced that it would stop servicing third-party cookers—cookies in the Chrome browser. Google's announcement said that the purpose of this was to protect consumers and to protect their data.

Left unsaid was how this could impact Google's ad tech competitors, and also left unsaid was the amount of information that Google collects from consumers—the browser data, location data, app usage data, financial transaction data, et cetera.

Tell me, how is it that consumers are any more protected if Google collects this data and your competitors can't? Can you help me understand that?

Mr. ERICKSON. Senator, thank you for the question. Yes, I can try. With the announcement that we made you rightfully point out that we would stop supporting intrusive tracking technologies like third-party cookies. We made the announcement in an effort to chart a course for a more privacy-enhancing web. We did not unilaterally withdraw our support for that but rather wanted to engage in a thoughtful conversation with advertisers, with publishers that rely on an ad-supported ecosystem to be able to function their websites or to reach consumers. We want to engage with regulators and governments and other stakeholders to explore more privacy-protective technologies, those are the intrusive technologies.

Senator LEE. Sir, I'm not sure you're grasping my question. You're at least not answering it. I appreciate that you're wanting to have a thoughtful conversation. I appreciate that you include this was in your business interest, and it may well have been. That's totally within your right. What I'm asking you to explain is your apparent assertion that consumers are any more protected if you collect that data and your competitors can't.

Mr. ERICKSON. Senator, so——

Senator LEE. That is your assertion, right? I mean that is the assertion that you made in that announcement. You said you're not going to service the third-party cookies in the Chrome browser, and——

Mr. ERICKSON. I'm sorry.

Senator LEE. Go ahead.

Mr. ERICKSON. Senator, we think the advertising ecosystem can thrive without having privacy-intrusive technologies like tracking devices or third-party cookies. The data that users—we are transparent with the collection practices that we have and the uses of our data, and we want to give consumers, and we do give them meaningful choice over the uses of their data, including to decide that they don't want to see targeted ads and relevant ads. They can choose not to see those or to mute ads that appear on third-party sites. There's many, many advertisers in the ecosystem. The access to data from consumers can be gotten from data brokers and other providers, so we don't think—the data in that regard is not viable. The data that consumers may provide with us are often provided to other online actors as well, and some of these companies are some of the biggest companies in the world. You implicitly raised a very important point, which is as we see regulators around the world push us and others, rightfully so, to have more privacy-protective technologies and to chart a course through a more privacy-centric web. There are competitors out there that are urging competition authorities to have us make more personally identifiable information released to the ecosystem.

We think that—we want to engage in these conversations. We think we can have a privacy-centric web while ensuring consumer

choice and competition, and that publishers and advertisers will continue to be able to have a business model that allow them to provide their websites and services to consumers in the way they do today.

Senator LEE. Okay, yes, I understand that. Look, I get the fact that you can always point to areas where things could get worse. Mandatory disclosures of personally identifying information on the web or otherwise. It is rather significant here that these things that you're talking about, steps that you've taken to exclude would-be competitors from the marketplace in circumstances in which Google's happy to provide advertisers with an alternative making them more dependent on Google, or it does in pretty much your bottom line.

Ms. Slaiman, do you agree with Google's statement? Are consumers better off with only Google being able to collect these types of data?

Ms. SLAIMAN. No, I don't agree with that statement. I don't think that users' privacy is improved, and I think it's a problem for competition. I really think we're being presented here with a false choice. There's another alternative, which is that some of this data should not be tracked at all.

Senator LEE. Sounds like you agree with my reluctance to accept the premise that people are safer because of this. I just realized I'm dangerously over time. Chairwoman Klobuchar has been very indulgent. I apologize. Thank you.

Chair KLOBUCHAR. Thank you. Next up Senator Cruz. Thank you.

Senator CRUZ. Thank you, Madam Chair. Mr. Satterfield, my questions will be for you. Last week, the Wall Street Journal ran a damning article entitled, "Facebook Knows Instagram Is Toxic For Teen Girls, Company Documents Show." The tagline below it was quote, "Its own in-depth research shows a significant teen mental health issue that Facebook plays down in public."

I know about this article because my wife, Heidi, who reads the Journal every day said, "You need to read this article now." I read it word for word.

All of us know that these products are addictive and that companies like Facebook design them in this way in order to maximize addiction, to capture eyeballs, which captures data, which is then used to sell advertising. For years, Facebook has been publicly insisting that its products aren't harmful and particularly that they're not harming teenagers.

We now know that was a lie. Facebook knew that its products, and specifically Instagram, was destroying the lives of far too many teenage girls. Facebook knew this because Facebook conducted its own studies into how Instagram affected young users and found that Instagram is harmful to a sizable percentage of them.

In fact, a slide from 2019 summara—summarizing this research said quote, "We make body image issues worse for one in three teen girls." Another Facebook slide said quote, "Teens blame Instagram for increases in the rate of anxiety and depression." Another slide said quote, "Teens who struggle with mental health say Instagram makes it worse." Most egregiously, one presentation said that among teens who reported suicidal thoughts, 13 percent of

British users and 6 percent of America's users traded—traced their desire to kill themselves to Instagram.

This should've made Facebook stop dead in its tracks and ask what in the hell you were doing. Instead, Facebook publicly downplayed the risk to young users and committed to push, to make sure more at-risk teenage girls used Instagram because more users including more teenagers means more money, whatever the human cost.

This is appalling. The American people deserve a thorough investigation into Facebook's willingness and eagerness to mislead the public about the risks of their own products.

The Wall Street Journal article states that the research has been reviewed by top Facebook executives and was cited in a presentation given to Mark Zuckerberg.

Mr. Satterfield, is this accurate? Did Mark Zuckerberg have personal knowledge of this Facebook research?

Mr. SATTERFIELD. Senator, I don't know the answer to that question, but, you know, to your other points, I would strongly disagree with the notion that our products are unsafe. I strongly believe they are safe——

Senator CRUZ. Let me ask you. Did you have knowledge of this research, Mr. Satterfield?

Mr. SATTERFIELD. I'm sorry, Senator. I've read the Wall Street Journal article——

Senator CRUZ. Did you have knowledge of it before the Wall Street Journal article?

Mr. SATTERFIELD. Senator, I'm generally aware that we do research on our products.

Senator CRUZ. Are you familiar with this research?

Mr. SATTERFIELD. I wasn't familiar with this research outside of the context of the Journal article, no.

Senator CRUZ. Wait a second. Your title is vice president of privacy and public policy, and you had no idea about Facebook's own research showing that you're violating the privacy and destroying the lives of teenage girls. You didn't know about it? Is that what you're testifying today?

Mr. SATTERFIELD. Senator, we're a large company, we have a lot of teams working on a lot of different issues. I don't work on these issues, safety and well-being.

Senator CRUZ. You didn't know about it?

Mr. SATTERFIELD. I didn't. Other people did. We're happy to connect——

Senator CRUZ. You have zero knowledge whether Mark Zuckerberg knew about it or not?

Mr. SATTERFIELD. I—Senator, I don't know that. I don't know.

Senator CRUZ. You knew you were coming to testify in this hearing. I'm going to guess you read the Journal article before you showed up to testify?

Mr. SATTERFIELD. Senator, I came here to testify on data issues and antitrust——

Senator CRUZ. Did you read the Journal article before you showed up to testify?

Mr. SATTERFIELD. Senator, yes, I've read the Journal article.

Senator CRUZ. Okay. Presumably, you prepared for today's testimony, yes?

Mr. SATTERFIELD. Yes, Senator, I prepared.

Senator CRUZ. Did that preparation involve enquiring whether the Wall Street Journal was accurate when it said Mark Zuckerberg was aware of this research?

Mr. SATTERFIELD. Senator, I can't get into the issues that we discussed during prep with my lawyers.

Senator CRUZ. Why not? You're here testifying on behalf of Facebook. I'm asking whether you inquired, whether the Journal was right, that Zuckerberg knew about this research? Did you inquire about it, or did you remain willfully blind and not want to know if Zuckerberg knew about it?

Mr. SATTERFIELD. Senator, respectfully, I'm here to testify about data and antitrust issues. I don't work on these issues. I'm happy to put you in touch with the folks that do——

Senator CRUZ. Again, you're the vice president of privacy and public policy and so putting in place policies that result in more teen suicides, that does not fall within your purview?

Mr. SATTERFIELD. Senator, I don't agree with that characterization. I work on privacy. There are many people that work on these issues at the company.

Senator CRUZ. Okay. Let's take the specifics of Facebook's research. I read a quote a minute ago, quote, "We make body-image issues worse for one in three teen girls." I didn't write that. Facebook wrote that. Is that an accurate statement?

Mr. SATTERFIELD. Senator, we do this research in order to inform hard conversations that we have at the company.

Senator CRUZ. I didn't ask why you did the research. I asked if the statement that was the result of your research is true?

Mr. SATTERFIELD. Senator, this is the research that was discussed in the Journal. This is research that we did internally.

Senator CRUZ. Was that a conclusion of your research? Yes or no?

Mr. SATTERFIELD. Senator, I'm aware of the Wall Street Journal article. I've read the Wall Street Journal article which discusses the research.

Senator CRUZ. All right. Let's try another conclusion. The Facebook research concluded that 13 percent of British users and 6 percent of American users trace their desire to kill themselves to Instagram. Is that a conclusion of your research?

Mr. SATTERFIELD. Senator Cruz, respectfully, we have teams that work on these issues. I'm not on those teams. We would be happy——

Senator CRUZ. Respectfully, you're not answering the question. It's a simple binary question. Did your research conclude that or not? If it's not, show us the research that didn't conclude that? If it is, then the question is, "What's the culpability of a company that knows it is contributing to an expanding teen suicide?" Did your research conclude that six percent of American users trace their desire to kill themselves to Instagram? Yes or no?

Mr. SATTERFIELD. Senator, again, these aren't issues that I work on at the company. I'm happy to bring folks in for a briefing with you and your staff.

Senator CRUZ. I understand that you would prefer a briefing without the public being aware of it, but I'm the father of two girls, including a teenage girl. Let me ask you something. In your judgment, in the judgment of Facebook, is increased teen suicide an acceptable business risk?

Mr. SATTERFIELD. Senator, of course not.

Senator CRUZ. Has Facebook quantified how many additional teenagers took their life because of your products?

Mr. SATTERFIELD. Senator, again, with respect, these aren't the issues that I work on. I came here today to talk about data and antitrust.

Senator CRUZ. Let me ask you. What would you say to the parents of a teenager who took her own life because of your products? What would you say when, two years ago, you had research that you conducted that concluded your products would contribute to and expand teen suicide? What would you say to a parent on behalf of Facebook who was facing that horrific tragedy?

Mr. SATTERFIELD. Senator, obviously losing a child to a tragedy like that is devastating. I have children. I take these issues incredibly seriously myself.

Senator CRUZ. Does Facebook?

Mr. SATTERFIELD. Of course, we do, Senator.

Senator CRUZ. Then what did you do differently? You got these results two years ago. What conduct changed? You don't get to say you take these issues seriously if you continue doing exactly the same and profiting off of—off of applications that are endangering the lives of teenage girls. What did you do differently because of this research?

Mr. SATTERFIELD. Senator, we did this research to inform our decision-making. We have consistently made——

Senator CRUZ. Did anything change?

Mr. SATTERFIELD [continuing]. Improvements to the product——

Senator CRUZ. Did anything change?

Mr. SATTERFIELD [continuing]. To address issues like well-being. I would love to have a team come in——

Senator CRUZ. Did anything change?

Mr. SATTERFIELD. Senator, we've made changes to our products over the last, you know, 10, 12 years——

Senator CRUZ. Did anything change to reduce the risk of teen suicide because of your product? Did you read this research and say, "Oh, my God, this is horrifying. Let's change"? Did you do anything to change, or did you just say, "Hey, we're printing money so we're good with this"? Which one was it?

Mr. SATTERFIELD. Senator, I would love to have a team come and give you and your staff a full briefing on these issues. We have made significant——

Senator CRUZ. It's the American people who deserve a briefing.

Mr. SATTERFIELD [continuing]. To safety and security. I would love to share more about this with you with the folks who work on these things.

Senator CRUZ. The entire American people deserve to know the answers to these questions.

Chair KLOBUCHAR. Thank you very much. I'm going to finish up here with my second round of questions, and I want to bring us

back to the subject of the hearing on data, because we have some major opportunities to move, right now, legislation that I think will be very helpful.

The first I've mentioned, which is right in front of us before the House, the bill that Senator Grassley and I have to modernize the merger filing fees. We also have opportunities in this budget in reconciliation, and you know, my view is—and I guess I'll ask you this, Ms. Slaiman. The President can appoint aggressive enforcers. He can issue executive orders which was great, but if we don't have the resources to take on the world's biggest companies, is it going to all work?

Ms. SLAIMAN. Right. I think you're absolutely right, Madam Chairwoman. We need more funding for our antitrust enforcement agencies. Obviously, that alone is not going to be sufficient so I'm glad that you're working on a lot of other important pieces of the puzzle as well, but that's an important one that we ought to be able to get done.

Chair KLOBUCHAR. Okay. Very good. Then we have not seen a lot of antitrust enforcement against mergers or anticompetitive conduct based on the issue raised by what this hearing has for the most part focused on, which is data. It's clear that big data does raise complex competition issues, but I'm doubtful that when you see some of these court cases recently that in my mind have gone in the wrong direction to begin with, but then we have this complex area of data and what that means for dominant carriers with no new laws or adjustment of laws. That's why the Competition and Antitrust Law Enforcement Reform Act that I introduced with Senators Leahy, Blumenthal, Booker, and many others would update our laws.

Could you talk about how this would help to address competition issues raised by big data?

Ms. SLAIMAN. Yes. Thank you so much, Madam Chairwoman. I think that's absolutely right that recently, and not so recently—it's been going on for decades now—that our antitrust laws have been narrowed and narrowed by these court decisions. So, now that we are facing the difficult challenges of big data, it's very difficult to bring a case, for example, where innovation harms are an important part of, you know, what the agencies are trying to argue. I think it will be incredibly helpful to have your legislation in place that updates the legal standard both for mergers and for exclusionary conduct.

Exclusionary conduct in particular is how a lot of these big data concerns are happening, and it has really been difficult to bring exclusionary conduct to cases, which is a broader problem beyond big data, but it's particularly relevant here.

Chair KLOBUCHAR. Maybe we could talk a little bit about that, you know, the relevance of it.

As we look at privacy legislation, and I know, Mr. Satterfield, you talked about privacy legislation, and in your written testimony and past blog posts you've written about the need for Congress to enact it that could create rules to govern how platforms should use, analyze, and share data. What restrictions do you think the U.S. Government should put on targeted advertising, both from a privacy and competition perspective, and should such legislation be

limited to platforms like Facebook, Google, and Amazon, or should it apply to data brokers too?

Mr. SATTERFIELD. Thank you, Senator. We think the comprehensive privacy legislation is incredibly important for the Congress to take up and pass. In terms of who it should apply to, we think it should apply across the board to companies that process people's personal data. We think that it should have components like basic rights around your data, the rights to access, correct, delete and move your data to another service. We think that companies should be required to build internal processes to make sure that they're thinking about privacy when they build their products and services. I think that those are the basic components of the framework that we would advocate for.

Chair KLOBUCHAR. Anyone else like to comment on the rules the Federal Government should put in place to ensure the market for targeted advertising remains competitive, which is a little different than just privacy?

Ms. COLCLASURE. I'd like to jump in.

Chair KLOBUCHAR. Okay.

Ms. COLCLASURE. Say that I think we need an accountability-based law. We've been advocating for a Federal law for almost 20 years, and we believe it's very important for all Americans to have the same rights and for businesses to have predictability and certainty. The accountability construct is one that says it parses out, and this is especially important for digital advertising, that you should use data for benefit, for good purpose, and you are responsible and answerable, the accountability construct, for detecting and preventing harm.

I love what Senator Blumenthal said earlier, that data is an abstract of a person, and I believe it deserves all the dignity that we people should have. So when you process data, when you activate data for digital advertising, it's about fairness, not manipulation, and that's the way we govern data, and that's what we believe, and that's what we advocate for in addition to the basic rights. We parse privacy out. It's the right to an area of seclusion. Where can we as people be free, natural, unobserved humans? The right to agency. That's that choice, participation, control, access. Then the right to fair processing. That is the third piece of privacy and that is in the digital age.

The reality of digital is it's getting so complex people do not want to sit in front of a NASA space station control panel and say, "Yes, yes. No, no. Yes, yes." We have to get the defaults right, and it has to be that participants, all participants, are accountable for, "Do no harm" and "Do good things in service to people."

It is privacy by design. The computer code is the conduct. Thank you, Senator.

Chair KLOBUCHAR. Okay. Very good. Ms. Slaiman, you may want to add to that, but one of the goals of competition as to policy is to ensure there's a broad range of choices. If ads are targeted based on data companies have collected about each of us and the inferences they have made about our interest, does that raise concerns for you about consumers abilities to freely choose the products and services that are best for them, ranging from financial services, housing, healthcare, employment opportunities, and more, when

some of them are being targeted because of their data that they didn't really know they shared compared to other competitors?

Do you want to address that?

Ms. SLAIMAN. Yes, that's something that we're very concerned about. I do think that creates an opportunity for anti-competitive discrimination. It also creates an opportunity for discrimination, racial discrimination, and gender discrimination, and we've seen instances of that happening, so I think these are very serious harms that we need to be addressing.

To focus on the anti-competitive discrimination, I do think in addition to the consumer choice limitations, we're also concerned about the impact that this has on businesses. If a business is assessed by one of these algorithms to not be popular with a certain category of users, that can make things incredibly difficult for them because of the power of these platforms, because they occupy that gatekeeper role. It's much different than if a brick-and-mortar grocery store decides not to show your product, you can go somewhere else. With these gatekeeper platforms that's not a practical real option for companies. There's a variety of harms I think that come from that.

Chair KLOBUCHAR. Mr. Erickson, what is your company doing to ensure that competition is not being distorted by your targeted advertising systems with Google?

Mr. ERICKSON. Senator, thank you for the question. I think primarily consumers need to have transparency over their data, how data is being used, and meaningful choices about the use of that data. On the Google platforms, we provide an easy way for consumers to see exactly what data is stored relative to their account. They can delete that data if they want to. They can also make changes to say they don't want behavioral advertising targeted ads to them. They don't want to see—they want to mute ads on third-party sites, so I think the important thing here is to ensure that consumers have transparency and that they have meaningful choice, and we think privacy legislation should reflect those values as well.

Chair KLOBUCHAR. Okay. Earlier in my opening, I talk about Apple recently rolling out an update to its users, prompting them to agree or opt out of being tracked from across the apps they use. Early indications, as I noted, suggest a lot of them are doing it, something like 75 percent. Has Google considered doing something similar, including for its Android operating system?

Mr. ERICKSON. Senator, thank you. Google has announced that they will—we will stop supporting privacy-intrusive tracking technologies, like third-party cookies. At the same time, we've opened up a dialog through our Privacy Sandbox initiative to have a discussion with advertisers, with publishers, with governments, on how the industry can move to more privacy-enhancing, privacy-protective business models that still allow small businesses, website owners, to be able to have an ad-supported business and provide free products and services to consumers.

Chair KLOBUCHAR. Through the initiative the Privacy Sandbox initiative, you've mentioned some of these changes that you made to your web browser, Chrome.

However, from a competition perspective these changes have raised concerns that Google will still have access to detailed data, but others won't. How do you respond to those concerns?

Mr. ERICKSON. Senator, when we announced that we would cease support of these intrusive tracking devices, the third-party cookies, we also announced that we would not substitute those for alternative tracking mechanisms, but rather the idea behind the Privacy Sandbox was try to move as an industry toward more privacy, secure technologies that would still support an ad ecosystem but in privacy-enhancing ways.

Chair KLOBUCHAR. Do you want to respond to that, Ms. Slaiman, and then I'll just ask you the last question here?

Ms. SLAIMAN. Thank you so much. The Privacy Sandbox creates a situation where Google is still getting the data. They may call that privacy because fewer companies are getting the data, but Google is still able to fully exploit that data.

I don't think that that is giving users more privacy.

Chair KLOBUCHAR. Okay. My last question of you is about, you know, I've asked you some questions on the record, later, on mergers and things like that, and my bill, but just a kind of broad question here, Ms. Slaiman. In your opinion, do we need new laws to fully address the competition issues raised by big data, or can we just live with what we've got? That's called a softball.

Ms. SLAIMAN. [Laughter] Thank you so much. We absolutely need new laws, and that's something that we're working very hard on. I think we need to use all of the tools at our disposal, so we need to increase enforcement with the current laws that we have.

We need to push for rulemaking at the FTC with the current laws that we have, but at the same time, it is so important that we have improvements to the antitrust laws and sector-specific antitrust laws focused on big tech.

Chair KLOBUCHAR. Very good. I think that says it all. Do you want to add anything, Senator Lee? Oh, you do? Okay. Because we want to have a 4-hour hearing, not just three and a half, no. Go, I'm kidding. Go ahead.

Senator LEE. I can go for four and a half.

Chair KLOBUCHAR. No, that's okay. Why don't you just finish up here.

Senator LEE. I'll keep this brief. Mr. Satterfield, what's going to happen to the employees at Facebook involved in providing the leaked documents to the Wall Street Journal? Are they going to be retaliated against?

Mr. SATTERFIELD. Senator, I can't discuss H.R. issues in a public forum.

Senator LEE. Would it be appropriate for you to retaliate against them, assuming they broke no laws? Would it be appropriate for you to retaliate against them?

Mr. SATTERFIELD. No, Senator, of course not. Of course, it wouldn't be appropriate to retaliate against anyone.

Senator LEE. Will you issue a commitment to me that Facebook will not retaliate against them?

Mr. SATTERFIELD. Senator, yes. I'm happy to commit to that.

Senator LEE. That would be wonderful. Thank you. I appreciate that.

Chair KLOBUCHAR. Okay. I want to thank everyone for coming. There is a lot going on. We have a bill this week before the full Committee for markup on venues that Senator Lee and I have done together, the companion in the House. We have the funding bills and proposals that are very ripe for action right now. We have other bills that are tech-specific with Senator Blumenthal and Senator Blackburn and myself with the App Bill. We have interoperability proposals from the past, and then we have discrimination bills, anti-discrimination bills for exclusionary conduct and the like, that we're in the middle of right now, working on. The House, of course, has proposals, some similar to ours, some different, but we've been working closely with our counterparts, which is Representative Cicilline and Representative Buck.

Then also we have broader bills. We had a hearing on meatpacking and consolidation in the grocery area. We have a—which went—was very well attended with the full Committee here. Senator Lee and Senator Grassley have a broad bill on antitrust. I have another one with a number of co-sponsors. There are some similarities in the bill right, Senator Lee? Yes, there are.

We're also looking at that across industry lines about things that we can do that aren't just about tech, actually, that hit the fact that we're seeing consolidation across this country from everything from cat food to coffins.

It's not really good to end with the word coffin, so—although, you know, we're not too far from Halloween, but I just want to thank the witnesses and assure you that we continue to want to work with everyone, but we know we need change, that just keeping on going like we are and saying, "Everything is fine, and we trust you," and it's just not enough. You know, we're glad that these companies have been successful. We're glad they employ people, we truly are. I have a Fitbit. Senator Lee and I have compared some of our Fitbit data over the years. I'm not going to reveal that, although you guys already know it, so there.

And—but, at the same time, we believe in capitalism and encouraging capitalism and rejuvenating capitalism, and a lot of what's going on right now has the obvious privacy concerns, many of which you heard today with a lot of understandable emotion. But then there's also competition concerns that once you get so big and have so much dominance that there are these barriers to entry. They make it impossible to allow competition, and that, in turn, of course, in the long term allows for too much money in the same few hands. It allows for companies to start preferencing themselves, and while we've seen incredible developments in technology, we do not deny that, we'll never know of some of the new bells and whistles on privacy we might've seen if we didn't have Facebook buy Instagram or WhatsApp, if there'd been some control on that. It's one of the reasons that I support looking back in some of the most consolidating industries, just as we did during the days of the AT&T breakup, to figure out what we can do to make this area more competitive.

You're not going to find a more interested and energized Subcommittee than this one, as you could see from today, including some visitors that aren't even on the Subcommittee that we welcome. So, thank you.

We will keep the record open for—is it a week? Okay, very good.

Thank you to Mark and to Avery for their work, and Senator Lee and his staff. Do you want to add anything, Mike?

Senator LEE. Thank you.

Chair KLOBUCHAR. Okay. Thank you. The hearing is adjourned.

[Whereupon, at 5:28 p.m., the Committee was adjourned.].

[Additional material submitted for the record follows.]

Witness List
Hearing before the
Senate Committee on the Judiciary
Subcommittee on Competition Policy, Antitrust, and Consumer Rights

"Big Data, Big Questions: Implications for Competition and Consumers"

Tuesday, September 21, 2021
Dirksen Senate Office Building Room 226
2:30 p.m.

Mr. Steve Satterfield
Vice President, Privacy & Public Policy
Facebook, Inc.
Menlo Park, CA

Mr. Markham Erickson
Vice President of Government Affairs and Public Policy
Google, Inc.
Mountain View, CA

Ms. Sheila Colclasure
Global Chief Digital Responsibility and Public Policy Officer
IPG Kinesso
Little Rock, AR

Mr. John Robb
Author
The Global Guerrillas Report
Acton, MA

Ms. Charlotte Slaiman
Competition Policy Director
Public Knowledge
Washington, D.C.

Sheila Colclasure

Testimony to the Senate Judiciary Committee
Subcommittee on Competition Policy, Antitrust, and Consumer Rights

Big Data, Big Questions: Implications for Competition and Consumers
September 21, 2021

Executive Summary of Testimony

Sheila Colclasure is the Global Chief Digital Responsibility and Public Policy Officer for Kinesso, an IPG company. Sheila and IPG support national competition and data privacy laws that enable fair and open use of data, require accountability of companies that collect, process, share and use data, and ensure robust protection for individuals and their data.

Witness Background

As Global Chief Digital Responsibility and Public Policy Officer, Sheila leads the global data policy and digital responsibility strategies for Kinesso, ensuring that data and digital technology are used ethically and accountably across the enterprise and with its parent company, IPG, and their clients. This means ensuring data and technology are used in ways that serve people. She helps ensure practices operating at the leading edge of digital technology are consistent with principles of responsible, respectful, proportionate and fair data use. Sheila is responsible for public policy engagement with regulators, policy groups, clients and other key stakeholders globally, advocating for ethical advertising and marketing practices in ways that earn trust. She is an advisor on the development and deployment of Kinesso's data-driven and digital solutions and services. She is a trusted thought partner, advisor, and reputational champion for IPG companies.

Ms. Colclasure is a recognized global thought leader on applied data ethics, accountable data governance and human-centered digital responsibility. Sheila has extensive knowledge of laws and societal expectations governing the collection and use of information, with particular depth in the rapidly evolving data-driven advertising and marketing ecosystem. She is continuously sought out by policy makers, regulators and government agencies for her views on data integrity and how to address the complexity of operationalizing and harmonizing next-generation data governance for the global digital data-driven ecosystem. Sheila is a Presidential Leadership Scholar and was recognized by CSO as one of the "12 amazing women in security" (2017).

She is a frequent speaker and media interviewee and has advanced data leadership and policy with the marketplace, regulators and lawmakers in many fora, including the Department of Health and Human Services' Datapalooza, the Attorney General Alliance, Dublin Tech Summit, Global Data Transparency Lab, Information Accountability Foundation Digital University for Regulator Series, and Ibero-American Data Protection Network. Sheila has presented key talks at global events for the Consumer Electronics' Show, Forrester, adExchanger, International Association

of Privacy Professionals, Healthcare Information and Management Systems Society, Digital Advertising Alliance, American Bar Association and the Marketing Sciences Institute.

Sheila serves on the advisory board of the Information Accountability Foundation (IAF) and is corporate liaison to several industry standards-setting groups.

Testimony of Witness

1. Introduction of IPG

Kinesso, Acxiom and Matterkind, and our parent company, IPG, provide marketing services for many of the largest brands in the world. We believe that marketing done ethically, fairly and subject to accountability connects people to brand value, creates community, democratizes knowledge and access, and is a vital economic engine. This guardianship requires that marketing be done in a transparent, accountable, and trustworthy manner.

Taking a proactive approach to the ethical use of data is at the core of how we deliver products and services to our clients. We start with the application of the design principles of security, privacy, and ethical data use in the planning, engineering and deployment of our marketing products and services. This is our North Star, and our approach includes processes that facilitate security, compliance with data protection and privacy requirements, accountability, and the trusted use of data. We continuously seek ways to advance thought and practice leadership within the marketing and advertising industry.

2. The U.S. Economy Depends on Data for Innovation and Growth

a. Consumer Data and Technology Fosters Innovation, Transformation, and Growth

First and foremost, consumer data and technology are fundamental to the global economy. The United States is home to many of the most innovative data-driven and technology-enabled companies in the world. The U.S. is also home to large online ecommerce and social media platforms that combine the benefits of consumer data and technology, thereby changing the competitive landscape for publishers, advertisers and independent data providers. As data has become ever more central to the modern economy, multiple states in the US have adopted, or are considering, privacy laws that will significantly impact today's data-driven, competitive dynamics in ways that are both intended and unanticipated.

Rather than restricting consumer data usage in a manner that stifles innovation and picks economic winners and losers, we support national competition and data privacy laws that (i) enable fair and open use of data, (ii) require accountability of companies that collect, process, share and use data, and (iii) ensure robust protection for individuals and their data. It is vitally important for America to have national competition and data privacy laws that are well-balanced, future-fit, good for people, good for our economy, and good for America's globally competitive position. We cannot burden shift accountability to people, stifle innovation, or write laws that prevent fair, responsible, and accountable uses of data in critical ways that benefit American consumers and businesses alike.

For at least the past two decades, data driven companies in the U.S. have generated tremendous innovation, benefits for people, and benefits for our economy. Technological advances have improved Americans' lives, enabled consumers to perform more of their daily activities online,

and created more access for people to products, goods, services, and knowledge. The connected marketplace and economy became even more vital to American people during the COVID-19 crisis. This shift from brick and mortar to connected commerce was enabled by data, and as a part of this acceleration, generated increasing amounts of data. Given the breadth and depth of the connected ecosystem, it is fair to say that the health of the data ecosystem, and fair competition within that ecosystem, are critical to maintaining the economic leadership position of the United States.

Just a few examples of the dynamic innovation and competition in the digital ecosystem include:

- Connected Advertising: Innovation requires companies to try new things. Independent data providers and technology companies pioneered Internet advertising as we know it today. They invented real time online ad space auctions and developed the technology, standards, and protocols on which those auctions run today, powering much of the consumer-driven internet. This is now estimated by Statista to be a $378 billion market and projected to reach $646 billion by 2024, shaped and led by U.S.-headquartered companies. This advertising market is also the engine that enables the distribution of much of the valuable content online, which has put more information in the hands of more people than ever before. Connected advertising and independent data enables small businesses to compete in the connected marketplace and enables new market entrants to find audiences for their products and services.

- E-Commerce and Digital Payments: Fraud-detection and identity-verification tools, which enable online commerce, rely on robust and accurate data to protect businesses and consumers. These tools enable consumers to safely conduct transactions and make payments whenever, wherever, and however they want, with confidence that their identity and wealth will not be commandeered by online fraudsters. At the same time, companies that sell their goods online and companies that manage online payments must be able to detect fraud and confirm the identity of the consumers with whom they are doing business. The combination of technology and the free flow of consumer data across the internet are critical tools both for online commerce and payments and for companies providing those goods and services.

- Personalized Marketing: U.S. companies developed the all-in-one solutions that enable speakers and organizations to communicate directly with consumers via email, text, and other digital channels. The defaults on how information about people is used must be set at "benefits on" rather than "benefits off," while also enabling consumers robust rights to transparency, choice, and other important controls over their data. Laws and regulations should support, rather than stifle or block the fair, open and accountable flow of information, payments and commerce, across the internet.

The combination of technology and consumer data allowed publishers to benefit from their own content, advertisers to benefit from tailored ad placement and campaign measurement, and consumers to benefit from the new products and services whose emergence and growth was accelerated through more personally relevant advertising and messaging. As the market evolved though, online ecommerce and social media platforms have become increasingly dominant in the technology aspects, audience aspects, and control of the online advertising marketplace that enables the connected marketplace. The size, volume and control of consumer data generated within their platforms may create natural limits on the ability of third parties to curate audiences, serve their own customers, and compete in and benefit from that marketplace.

b. Independent Data Providers Play a Key Role

Independent data providers play a key role in maintaining the competitive, vibrant, and innovative technology and data ecosystem the U.S. now enjoys. They collect consumer data from a variety of sources and make it available to other companies, subject to contractual protections, for responsible uses. This facilitates commerce and innovation that drives value for citizens and companies alike.

A good example of the power of combining consumer data and technology is customer relationship management (CRM) systems, which are virtually ubiquitous in corporate America. These systems allow companies to know who their customers are and manage customer needs and preferences on an individualized basis. Similar systems have been developed in other arenas (such as HR and marketing) to identify and communicate with individuals (who may be employees or prospects), manage their preferences and satisfy their requirements. Without accurate, robust and curated consumer data though, these technologies are unable to identify relevant individual citizens, develop appropriate communications for a particular citizen, and measure the effectiveness of those communications, while at the same time implementing the citizen's privacy, communications and data preferences.

3. Privacy Laws Should Be Drafted to Enhance the Flow of Responsibly Sourced Data Which Fosters Innovation and Competition.

Regulatory approaches to privacy thus far have not considered the potential impacts of data use restrictions on competition. Instead, U.S. and EU privacy laws have taken a "pure privacy" approach, with the apparently singular goal of further restricting use of consumer data. Responsible data collection and use is critical for citizens. Such principles must be implemented in a manner that promotes innovation and competition. This is best explored by considering (a) why data is important for competitive markets, (b) the (perhaps unintended) anti-competitive consequences of laws that focus myopically on data use restrictions, and (c) U.S. merger policy that impacts data-driven markets.

a. Data Sharing is Key for Competition because Data is "Non-Rivalrous"

Data sharing is particularly important at the intersection between privacy and competition. Data is what economists call a "non-rivalrous good." Company A and Company B can use the same data set at the same time. It is fundamentally different than a physical asset, such as a pair of shoes – if one person is wearing the shoes, no one else can wear them.

The ability to share data, rather than limiting its use to only one entity, thus simultaneously supports both innovation and competition. Independent data providers, for instance, can provide accurate, lawfully gathered and maintained consumer data to multiple companies, for responsible, fair, and legitimate uses. Multiple companies, for instance, can draw on a consumer data set to reduce fraud, and use that same data to advertise useful products and services, resulting in better service to people, and better economic and communications results. Those companies then compete against one another, but only to the extent they each have sufficient access to consumer data with which to do so.

When dominant players are able to maintain exclusive control over vast amounts of consumer data, it tends to enhance their market power and create barriers to entry. Exclusive control over data can provide an incumbent with critical economies of scale and scope, allowing them to raise product quality and attract consumers at lower cost than competitors. In contrast, lack of access

to that data constitutes a barrier to entry, expansion and innovation by smaller competitors. As the influential Stigler Committee on Digital Platforms observed in 2019, exclusive control over data tends to make the strong stronger and the weak weaker.[1]

Rules that unreasonably restrict the use or sharing of consumer data can exacerbate these concerns by transforming data into a rivalrous good. The General Data Protection Regulation adopted by the EU in 2018 (commonly known as the GDPR) gives preferential treatment to "first parties" – a company that collects consumer data directly from a consumer. The GDPR sets strict limits on beneficial consumer data uses by "third parties," such as companies that rely on consumer data they receive from independent data providers. The GDPR rules give the first parties control of consumer data. These are often larger and entrenched competitors who are given a major competitive advantage over third parties who may be smaller or nascent competitors. Under this regulatory approach, a company's position in the data ecosystem can perhaps outweigh its ability to innovate and provide better products and service.

b. The GDPR Experience Shows the Potential Negative Effects of Privacy Laws on Competition

The evidence is now in. The GDPR has harmed competition in the name of privacy protection. While it has increased protections for personal data in the EU, it has simultaneously undermined competition, and this has entrenched the dominant players in many online markets.

According to multiple observers, the GDPR helped the largest platforms become more dominant, while making it more difficult for smaller companies and new market entrants to survive. The Wall Street Journal[2], Politico,[3] and the New York Times[4] have all reported that the GDPR primarily benefitted Google and Facebook, while hurting smaller competitors in the online advertising industry. A survey conducted by Ghostery and Cliqz, two providers of cookie-related services, found widespread belief that "Google is the biggest beneficiary of the GDPR," while third parties, such as smaller and mid-sized online advertising companies, were the biggest losers.[5]

Academic experts Michal Gal and Oshrit Aviv have written the most comprehensive study of the effects of GDPR on competition. They wrote in 2020:

---

[1] STIGLER COMM. ON DIGITAL PLATFORMS, FINAL REPORT at 40 (2019), available at https://research.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler%20center.pdf ("Barriers to equivalent data resources, a side effect of not having the history, scale, or scope of the incumbent, can inhibit entry, expansion, and innovation. The same effects that drive the quality of digital services higher as more users join—a positive feedback loop—makes the strong stronger and the weak weaker.").

[2] Nick Kostov & Sam Schechner, *GDPR Has Been a Boon for Google and Facebook*, WALL ST. J. (June 17, 2019), available at https://www.wsj.com/articles/gdpr-has-been-a-boon-for-google-and-facebook-11560789219.

[3] Mark Scott et al., *Six Months in, Europe's Privacy Revolution favors Google, Facebook*, POLITICO.COM (Nov. 23, 2018), available at https://www.politico.eu/article/gdpr-facebook-google-privacy- data-6-months-in-europes-privacy-revolution-favors-google-facebook/.

[4] *How Facebook and Google Could Benefit from the G.D.P.R.*, NEW YORK TIMES (Apr. 23, 2018), available at https://www.nytimes.com/2018/04/23/technology/privacy-regulation-facebook-google.html.

[5] Björn Greif, *Study: Google is the Biggest Beneficiary of the* GDPR, CLIQZ.COM (Oct. 10, 2018), available at https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr.

> The GDPR creates two main harmful effects on competition and innovation: it limits competition in markets, creating more concentrated market structures and entrenching the market power of those who are already strong; and it limits sharing between different collectors, thereby preventing the realization of some synergies which may lead to better data-based knowledge.[6]

After studying the effects of GDPR, Professors Gal and Aviv report that these limits on competition help explain "troubling empirical evidence regarding investment in EU data-driven markets following the adoption of the GDPR," finding that the new law has had unintended effects on competition, efficiency, and innovation.

The findings of Professors Gal and Aviv are consistent with the analysis that consumer data is a non-rivalrous good. Their position is that the GDPR limits data sharing between data collectors, blocking the useful sharing of data. They further assert that the GDPR limits competition in data markets, because the law entrenches the first parties in their position of market dominance.

In short, if privacy laws focus myopically on restricting data collection and sharing, while ignoring the potential effects on competition, they are likely to harm the very citizens they set out to protect by entrenching dominant players and undermining competition and innovation. Congress should consider privacy laws that permit beneficial forms of data sharing while (a) increasing transparency, (b) regulating sensitive or harmful uses of consumer data, and (c) imposing accountability on companies that collect, hold, and transfer data.

c. Mergers Can have Anticompetitive Effects in Data-Driven Markets

Mergers have been a key part of the strategy for many of the largest companies in the U.S., including the largest digital platforms, to achieve their current market position. For years, it appeared that regulators did not perceive that these acquisitions posed a threat to competition or innovation.

For example, in 2007, Google received antitrust clearance to purchase DoubleClick, then the market leader in display ads on the internet. Later, Facebook was permitted to purchase Instagram, before the latter could become a competitor at scale in the social media space.

There are, however, signs of change. Late last year, for example, the Federal Trade Commission (FTC) brought suit against Facebook, alleging that it maintained its monopoly in personal social networking through a years-long course of anticompetitive conduct, including its acquisitions of WhatsApp and Instagram.[7] And just last week, the FTC took two steps that suggest a renewed commitment to aggressively scrutinizing acquisitions in data-driven markets. First, the FTC released a report in which it analyzed a decade's worth of acquisitions by large digital platforms that were too small or otherwise exempt from reporting requirements under the Hart-Scott-Rodino Act.[8] FTC Chair Lina Khan explained that in light of the report's findings, the FTC will closely

---

[6] Michael Gal & Oshrit Aviv, *The Competitive Effects of the GDPR*, 16 J. OF COMPETITION L. & ECON. 349 (May 18, 2020), available at https://academic.oup.com/jcle/article-abstract/16/3/349/5837809?redirectedFrom=fulltext.

[7] A timeline of the FTC's action against Facebook, including links to the FTC's complaints, can be found at https://www.ftc.gov/enforcement/cases-proceedings/191-0134/facebook-inc-ftc-v.

[8] *See* Fed. Trade Comm'n, *Non-HSR Reported Acquisitions by Select Technology Platforms, 2010-2019: An FTC Study* (Sept. 15, 2021), available at https://www.ftc.gov/system/files/documents/reports/non-hsr-

examine reporting requirements to close reporting loopholes that she said may have allowed certain deals to "fly under the radar."[9] Second, the FTC voted to withdraw the Vertical Merger Guidelines just over a year after they were published. In doing so, the majority of the Commission promised to offer a new framework for vertical merger analysis that better takes into account the features specific to digital markets, including the potential for transactions to enable firms to exclude rivals by "degrading interoperability, reneging on access policies, or gaming algorithms."[10]

And, as this Committee knows, there are also a variety of legislative proposals before Congress that would make significant revisions to U.S. merger laws, including some that revise the standards for merger reviews or even bar some transactions altogether.[11]

Countries such as Germany have already amended their competition laws to provide more flexibility to address data-related issues. In Germany, Facebook was not subject to merger review when it purchased WhatsApp. Even though Facebook paid $19 billion to acquire WhatsApp, the merger controls did not apply because of the low amount of revenue WhatsApp generated at that time. Since then, Germany has implemented changes to permit regulatory scrutiny of acquisitions at lower revenue thresholds.

Given the importance of data to the economy and to consumers, we welcome efforts by enforcers and Congress to carefully consider appropriate steps to ensure that competition in data markets is unfettered and vibrant and that future acquisitions do not improperly stifle new entry and innovation.

4. How Privacy Legislation Can Foster Innovation and Competition

We encourage the Committee to consider privacy and competition not as separate bodies of law, but instead to be interrelated. Privacy laws materially impact markets, so they should be drafted to foster innovation and competition, not simply to increase data control and potential resulting concentration.[12] Antitrust laws impact citizen privacy, so they should be drafted to protect citizens

---

reported-acquisitions-select-technology-platforms-2010-2019-ftc-study/p201201technologyplatformstudy2021.pdf.

[9] *See* Fed. Trade Comm'n, *Remarks of Chair Lina M. Khan Regarding Non-HSR Reported Acquisitions by Select Technology Platforms*, Comm'n File No. P201201 (Sept. 15, 2021), available at https://www.ftc.gov/system/files/documents/public_statements/1596332/remarks_of_chair_lina_m_khan_regarding_non-hsr_reported_acquisitions_by_select_technology_platforms.pdf.

[10] *See* Fed. Trade Comm'n, *Statement of Chair Lina N. Khan, Comm'r Rohit Chopra, and Comm'r Rebecca Kelly Slaughter on the Withdrawal of the Vertical Merger Guidelines*, Comm'n File No. P810034 at 7 (Sept. 15, 2021), available at https://www.ftc.gov/system/files/documents/public_statements/1596396/statement_of_chair_lina_m_khan_commissioner_rohit_chopra_and_commissioner_rebecca_kelly_slaughter_on.pdf.

[11] *See, e.g.,* the Competition and Antitrust Law Enforcement Reform Act of 2021, S. 224, 117th Cong. (2021), available at https://www.congress.gov/bill/117th-congress/senate-bill/225/text; and the Trust-Busting for the Twenty-First Century Act, S. 1074, 117th Cong. (2021), available at https://www.congress.gov/bill/117th-congress/senate-bill/1074. For a bill introduced in the House, *see* the Platform Competition and Opportunity Act, H.R. 3826, 117th Cong. (2021), available at https://www.congress.gov/bill/117th-congress/house-bill/3826/ (would prohibit dominant platforms from acquiring competitive threats or engaging in acquisitions that would "increase or enhance" the platform's market position).

[12] Of significant note, the United Kingdom announced earlier this month that it was beginning a consultation process that would build on principles within the GDPR in order to "support vibrant competition and innovation to drive economic growth" and "maintain high data protection standards without creating

and require responsible and accountable uses of their data. America should focus on constructing future-prepared laws that support a fair, competitive, healthy, trustworthy, connected economy.

a. Accountability-Based Frameworks Support Innovation and Growth

Our economy depends in key part on companies' ability to readily access and share consumer data. We thus encourage the Committee to consider legislative approaches that do not severely restrict companies from collecting, using, or sharing consumer data. The economy is too complex, and consumer data practices are too multilayered, for statutes to pinpoint who should hold consumer data and who should not. That approach potentially determines which companies can compete, unfairly entrenching companies with more consumer data with a superior competitive position.

Instead, we encourage the Committee to consider a more balanced approach that focuses on imposing accountability on companies that use citizens' data. Accountability-based frameworks regulate sensitive or potentially harmful uses of consumer data, while permitting the pro-competitive data collection and sharing the U.S. economy needs for innovation and growth. For example:

- Accountability can require holders of citizens' data to build internal governance programs for protecting data, such as (a) implementing internal privacy policies and controls, (b) designating data privacy officer(s), and (c) documenting Privacy Impact Assessments before engaging in activities that present heightened risks to citizens. Governance requirements can be scaled so that larger data holders are expected to have more robust governance in place.
- These frameworks can also require companies to contractually bind service providers and third parties that receive consumer data to specified protective obligations.
- Emerging practices that carry risk for citizens – such as algorithm development – can be subject to additional assessment and reporting requirements.
- Companies that hold consumer data and are not immediately visible to consumers, such as independent data providers, can register with a regulator to enable consumers to know who they are.

Accountability-based frameworks can also be supplemented with transparency rules and individual control rights that consumers can exercise. These can include rights to access their consumer data, delete that data, or opt-out of specified types of data sharing.

b. Now is the Time to Act

In closing, the right view of the intersection of data and competition should lead to the right outcome for a national privacy law. Congress has a critical window to act on privacy legislation. In January 2023, California's Privacy Rights Act (CPRA) as well as the new Virginia privacy law will go into effect, followed by the new Colorado Privacy Act in July 2023.[13] We expect more state

unnecessary barriers to responsible data use." *See* United Kingdom Department for Digital, Culture, Media, and Sport, *Data: A New Direction* (Sept. 10, 2021), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1016395/Data_Reform_Consultation_Document__Accessible_.pdf.

[13] For the California Consumer Privacy Act and/or California Privacy Rights Act, *see* Cal. Civ. Code § 1798.100 *et seq.* For the Colorado Privacy Act, *see* Colo. Rev. Stat. § 6-1-1301 *et seq.* For the Virginia Consumer Data Protection Act, *see* Va. Code § 59.1-571 *et seq.*

privacy laws to pass next year. These statutes will significantly limit how consumer data can be collected and shared, and will have practical effects across our national economy. In particular, CPRA will make consumer data sharing more difficult for online advertising. Consumers will have a right to opt-out of all "sharing" of their consumer data for common types of online advertising. Further, CPRA suggests that companies that provide online advertising services may not be able to use customer data to improve their advertising services for all their customers.

These rules are likely to have GDPR-like anticompetitive effects. Companies that have large quantities of citizen data may be by largely unaffected by CPRA, since they do not have to "share" consumer data with anyone but themselves. But for smaller competitors, which are critical to a robust marketplace and the development of future innovative solutions, access to essential consumer data may be cut off. This would require advertisers, publishers and others to work with fewer, more dominant players in order to communicate and interact with consumers, likely in a more expensive manner – which leaves small businesses fewer options on how to reach out to consumers. That is not an outcome that is pro-consumer.

5. Conclusion

Consumer data and technology are critical to the national and international economy. We support the adoption of a well-balanced federal privacy law and competition laws and policies that provide critical protections for individuals and their data, and enable the responsible flow of consumer data among all accountable companies, in order to preserve and enhance the connected marketplace.

Written Testimony of Markham Erickson
Vice President of Government Affairs and Public Policy, Google

Senate Committee on the Judiciary
Subcommittee on Competition Policy, Antitrust, and Consumer Rights

"Big Data, Big Questions: Implications for Competition and Consumers"
September 21, 2021

Chairwoman Klobuchar, Ranking Member Lee, and distinguished members of the Subcommittee:

Thank you for the opportunity to appear before you today. My name is Markham Erickson. I am a Vice President of Government Affairs and Public Policy at Google. I have worked at the intersection of technology and policy for over 25 years, primarily in private practice where I had the opportunity to work on issues that defined the evolution of the modern Internet. In my role at Google, I oversee a global team of subject matter experts focused on the application of law and policy to technology and the internet, including on issues related to data governance and competition.

We appreciate the topic of this hearing on the implications of data for competition and consumers. Data should be used to make consumers' lives better by improving the quality and diversity of products and services available,[1] while protecting users' privacy and giving them control over their data. In this testimony, I will describe (1) how Google uses and protects data; (2) how data mobility empowers consumers and boosts competition, including data portability and advancing open data; and (3) that data alone does not guarantee better products for consumers.

How we use and protect data

Data plays an important role in making the Google products and services people use everyday functional and helpful. We are committed to treating that data responsibly and protecting privacy with strict protocols and innovative privacy technologies.

[1] For example: Doctors can use data to improve patient outcomes, scientists rely on data to better predict weather, and governments rely on data to monitor things like the impact of the COVID-19 pandemic. And brick and mortar retail businesses reduce costs and connect with and help consumers through the innovative use of data.

Google combines insights from data with industry-leading technology to develop products that help people find directions, grow their businesses, or search for information. Google provides information about the personal data we collect and how we use it—such as to provide better services—to our users and the public. We provide notice not just through our privacy policy[2], but also through our work to actively inform individuals about data use in the context of the services themselves, helping to make the information relevant and actionable. On an individual level, what data is collected and how it is used depends on how each person uses our services and how they manage their privacy controls.

Data is one element of our advertising business, where it helps us connect people with relevant advertisements. Advertising is Google's main source of revenue, and enables us to make many of our flagship products, including Search and Maps, available for free to billions of people around the world.[3] Google's advertising platforms support businesses of all types and sizes by helping them reach customers. To give an example of what this means for small businesses, the owner of a local flower store, Studley Flowers in Rochester, New Hampshire said, "Google Ads has provided us with a cost-effective way to compete with the national flower delivery brands and their larger ad budgets. Additionally, it provides us with a way to make sure that when locals search for flowers, we stay top of mind against those larger brands. Our investment in Google tools has certainly paid off, and we're excited to see what's next."[4]

Google also helps millions of website publishers earn advertising revenue on their sites and apps. The ads shown are informed by a search query or page content, but can also be based on a user's interests or other personal data if their privacy settings permit.[5] We do not sell our users personal information to advertisers, or to anyone else.

Our business relies on ensuring our users' trust, specifically in how we use and protect their data. We do this in part by offering industry-leading controls to manage privacy and empowering users to adjust what data is stored in their Google Account. Three billion users visit their Google accounts every year, where they can review and change their privacy settings and delete data stored in their account. For example, Google

---

[2] https://policies.google.com/privacy?hl=en-US
[3] https://about.google/intl/en_US/how-our-business-works/
[4] https://partnertestimonials.withgoogle.com/?_ga=2.19953275.2136290102.1632085855-932915823.1630594247#q[15]
[5] https://howwemakemoney.withgoogle.com/

users can always turn off personalized ads[6] in their Account Settings[7] while still using Google products for free. And since 2019,[8] we have offered industry-leading auto-delete features that give our users the option to automatically delete data from their account, like their Search History. Starting in 2020,[9] new accounts auto-delete some account data by default after 18 months. We regularly prompt our users to review and manage their privacy and security settings with emails and promotions on the Google homepage.

We also invest in research and development of cutting-edge privacy and security engineering techniques that are applied in our products. We share a range of these innovative tools in open source formats, which are free for anyone—including competing companies—to use, benefitting the broader ecosystem. For example, Google's differential privacy library has been used by hundreds of developers around the globe to gain insight from data while protecting individual privacy.[10]

In addition to putting users in control, we keep their data secure by default. Every day, we block 100 million phishing attempts and 15 billion spam messages in Gmail and encrypt four billion photos[11]. Our free Safe Browsing[12] tool helps keep the rest of the Internet secure, automatically protecting more than four billion devices every day by showing warnings to users when they attempt to navigate to dangerous sites or download dangerous files.

We constantly innovate to improve privacy across our own products and on our platforms. This sometimes means finding ways to reduce the amount of personal information needed to achieve similar outcomes. For example, we recently announced Privacy Sandbox, a collaborative initiative that aims to help build a more private and secure web. Through the Sandbox initiative, we are working with the ads industry to develop new digital advertising tools that protect people's privacy and prevent covert tracking, while continuing to support an open and free Internet enabled by advertising. From the start of this project, we developed these tools in an open manner, and sought feedback from industry partners, civil society, and governments. Because many publishers and advertisers rely on online advertising to fund their websites to connect

[6] https://support.google.com/accounts/answer/465?hl=en&co=GENIE.Platform%3DDesktop
[7] https://support.google.com/ads/answer/2662856?
[8] https://blog.google/technology/safety-security/automatically-delete-data/
[9] https://blog.google/technology/safety-security/keeping-private-information-private/
[10] https://developers.googleblog.com/2019/09/enabling-developers-and-organizations.html
[11] https://blog.google/technology/safety-security/our-work-keep-you-safe/
[12] https://safebrowsing.google.com/

with customers, getting this balance right is key to keeping the web open and accessible to everyone. We are proud of our work to apply innovative solutions that balance these interests.

Data mobility empowers consumers and boosts competition

There are considerable options to use available data safely, including tools and resources from Google. Data can be transferred safely in two ways: personal information can be moved from one service to another based on a specific individual's instruction, and datasets can be shared safely as open data using appropriate privacy technologies.

Data portability

Google has been a leader on data portability for over a decade, enabling our users to export their data and take it to another platform. Google's approach to data portability is simple: the user comes first.[13] Data portability empowers consumers to choose services or online platforms based on quality and individual preference—not because they are locked in or because they can not move their data to alternatives.

Since 2011, Google Takeout[14] has allowed users to export their data from over 70 Google products and download them in machine-readable formats so that they can be easily uploaded to another service. Takeout makes it possible for users to move their content to competing services,[15] so no one feels they have to continue using Google if they prefer a service of another company. Since our launch of Takeout, users have exported more than one billion gigabytes from Google products.[16]

Additionally, through our leadership in the Data Transfer Project,[17] Google makes it easier for companies of all sizes to provide tools that let users move data between online services. The Data Transfer Project, a partnership among Google, Apple, Facebook, Twitter, Microsoft, and Smugmug, supports the direct transfer of data between providers, allowing consumers to seamlessly and securely transfer their data directly from one provider to another, rather than downloading and re-uploading their

[13] https://publicpolicy.googleblog.com/2009/09/introducing-dataliberationorg-liberate.html
[14] https://takeout.google.com/u/0/settings/takeout
[15] https://support.google.com/accounts/answer/3024190?hl=en
[16] https://www.regulations.gov/document?D=FTC-2020-0062-0011
[17] https://datatransferproject.dev/

content. The code available through the Data Transfer Project reduces the engineering work any individual company has to do to offer portability to their users.[18]

Data portability benefits both consumers and competition. Giving users control over their data through easy-to-use data export tools boosts competition by reducing the burden of switching services. It paves the way for innovative and new opportunities for service providers of all sizes, and empowers people to try new services and choose the offering that best suits their needs.

Advancing open data and AI for All

Artificial intelligence (AI) is a transformative technology, and we are committed to making it accessible to more people and institutions. Google is a leader in releasing public data and tools that support advanced technological applications like machine learning (ML) and AI.

Many of the largest successes in machine learning have come from data that is openly available on the web. Google has released over 80 labeled datasets for ML researchers and developers to use.[19] For example, we open sourced the Open Images dataset to provide developers with geographically diverse images to support more inclusive results for underrepresented cultures in ML models. And through TensorFlow—an ecosystem of tools, programming libraries, and community resources—we are enabling developers from startups, large companies, and nonprofits to more easily use ML to build a variety of applications, from fraud detection in digital payments to online English grammar correction.[20] TensorFlow has more than 200,000 users and over 160 million downloads, and supports over $15 billion in economic impact in industries including computer manufacturing and software publishing.

In some cases, data that is already publicly available is hard to use because it is hard to find. Google has developed cutting edge tools to address this issue.[21] For example, Google pays for storage of, and provides public access to, public data available through Google Cloud Public Dataset Program.[22] Kaggle makes data science easier by providing all the code needed to leverage over 80,000 public datasets.[23] We also launched a search engine for datasets called Dataset Search.[24] Using a simple keyword

[18] https://www.regulations.gov/document?D=FTC-2020-0062-0010
[19] https://ai.google/tools/datasets/
[20] https://www.tensorflow.org/
[21] https://www.blog.google/technology/ai/sharing-open-data/
[22] https://cloud.google.com/solutions/datasets
[23] https://www.kaggle.com/datasets
[24] https://datasetsearch.research.google.com/help

search, users can discover datasets hosted in thousands of repositories across the Web.[25]

Google also makes insights from our data publicly available in privacy-safe formats, contributing to important research around the world. For example, Google Trends[26] was launched in 2006 and provides access to a largely unfiltered sample of actual search requests made to Google. It is anonymized (no one is personally identified), categorized (determining the topic for a search query), and aggregated (grouped together). Google Trends is a powerful tool for researchers, journalists, and civil society. There are more than 21,000 research papers on Google Scholar that cite Trends as a data source. [27]

During COVID-19, we have leveraged our expertise in open data and privacy to support governments, health officials, researchers, nonprofits, and others to understand the changing conditions around the pandemic. For example, Google provides a public repository of open-source data related to the global response to the novel coronavirus.[28] This includes epidemiology and health datasets, as well as data on government responses. We also share a privacy-safe version of Google's own mobility data. Google launched the COVID-19 Community Mobility Reports[29] in April of 2020.[30] These reports provide aggregated, anonymized mobility data. They use differential privacy to protect our user data, adding artificial noise to our datasets and enabling high quality results without identifying any individual person.[31] The reports have helped governments around the world understand how social distancing measures are influencing outcomes.

Companies of all sizes utilize code, tools, and knowledge sharing in open source platforms to support their product development. Google is one of the largest contributors to open source code to GitHub, a popular repository for software development tools.[32] In 2020, Googlers made more than 240,000 contributions to tens

[25] With this data, computer vision researchers can train image recognition systems. Waze for cities (https://www.waze.com/en-GB/wazeforcities) datasets are to inform mobility projects and policies, from congestion to event-specific traffic controls. Alphabet's Waymo Open Dataset (https://waymo.com/open/about/) contains high resolution sensor data collected by Waymo self-driving cars to aid the research community in making advancements in machine perception and self-driving technology.
[26] https://trends.google.com/trends/
[27] https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=%22google+trends%22&btnG=
[28] https://cloud.google.com/blog/products/data-analytics/publicly-available-covid-19-data-for-analytics
[29] https://www.google.com/covid19/mobility/
[30] https://blog.google/technology/health/covid-19-community-mobility-reports/
[31] https://support.google.com/covid19-mobility/answer/9825414?hl=en&ref_topic=9822927
[32] https://github.com/google

of thousands of projects on GitHub.[33] Google's open source work includes AI building blocks, data processing tools to process data including TensorFlow Privacy,[34] and models for language understanding and computer vision. All of these contributions make it easier for new and existing companies to develop and bring new products to consumers.

Data alone does not guarantee better products for consumers

Consumers have many choices over where they share their data—and they can and do choose to share the same data with multiple providers. In our experience, data by itself does not guarantee better or more successful products. It is the investment, innovation, and method that matters most.

Cutting edge technology or new ideas allows new companies to succeed, sometimes without any data at all. New entrants such as Zoom, Snapchat, Spotify, or Pinterest have been successful because they provide an innovative product, not because they have access to data from established companies.

Conversely, having more data does not itself guarantee success. Many businesses have had access to data but have had products that struggled to succeed.

Drawing insights from raw or aggregated data, including publicly available data, is where a company can add particular value to consumers and businesses. The process of using information and feedback to improve products and services is not unique to Google or the online world—it takes place across all sectors of our economy, where data helps firms improve and innovate and better serve consumers. It is what a company makes of the data, not how much data they have or use that determines their ability to innovate and succeed, and better serve their customers.

For example, data is just one component of what makes Google Search a useful product for users and businesses. To deliver Search results, Google's systems sort through hundreds of billions of webpages in our Search index to find the most relevant and useful results for our users. The publicly available web is an important data set to make that happen and we also have invested in indexing a wide range of information

---

[33] https://opensource.googleblog.com/2021/08/metrics-spikes-and-uncertainty-open-source-contribution-during-a-global-pandemic.html

[34] https://blog.tensorflow.org/2019/03/introducing-tensorflow-privacy-learning.html

from images, books, research papers, and much more to help our users understand the world's information.[35]

We know we need to keep innovating to find new ways for Search to deliver more useful information faster and more conveniently to consumers. In 2020, we ran over 600,000 experiments that resulted in more than 4,500 improvements to Search.[36] Improving our product involves steps as seemingly simple as a synonym system that allows us to find relevant documents even if they do not contain the exact words a user typed. For example, a user may search for "change laptop brightness" but the manufacturer has written "adjust laptop brightness." Our systems understand the words are related and are able to connect users with the right content. This system took over five years to develop and significantly improves results in over 30% of searches across languages.[37]

Our focus on continually improving our products means that our greatest source of innovation comes from extensive research and development (R&D). Last year alone we spent $27.6 billion on R&D, nearly ten times what we spent in 2009.

Advancements in AI and machine learning increasingly support ways to minimize the use of data while continuing to deliver and improve helpful products people rely on every day. For example, Google has been a leader in federated learning, a machine learning approach that learns from a user's interaction with a given device while keeping all the training data on the device, so that the data does not need to be shared with a server.[38] More recently, Google published research on Entities as Experts AI,[39] that answers text-based questions with less data.

Conclusion

We appreciate the opportunity to share our views on the implications of data for consumers and competition.

---

[35] https://www.google.com/search/howsearchworks/how-search-works/organizing-information/
[36] https://www.google.com/search/howsearchworks/how-search-works/rigorous-testing/
[37] https://www.google.com/search/howsearchworks/how-search-works/ranking-results/
[38] https://ai.googleblog.com/2017/04/federated-learning-collaborative.html
[39] https://venturebeat.com/2020/04/20/googles-entities-as-experts-ai-answers-text-based-questions-with-less-data/

We recognize policymakers and regulators are working to protect privacy while also considering arguments by those who contend that making more data available among competitors would increase competition. These complex discussions involve defining the types of data at issue, as well as identifying the types of services that use data, and the data necessary to make those services useful. We are encouraged to see some privacy and competition regulators conferring more formally to contribute their relevant expertise to the important questions being considered, for example when a privacy practice is being evaluated in an antitrust context. We will continue to engage with policymakers and regulators, as well as other stakeholders, to support thoughtful regulation that encourages innovation and protects consumers. For example, we have long supported federal privacy legislation in the U.S.[40]

We are committed to protecting data through privacy, security, and user control, and to continuing to improve our products in a way that ensures more choice and competition. We look forward to engaging with this Committee on these important issues.

Thank you for the opportunity to discuss our work today.

[40] https://blog.google/competition/#facts

Global Guerrilla Special-Report
Senate Testimony
September 2021

John Robb

Making Big Data Work for Us

Big Data has become central to economic and social progress in the 21st Century. Depending on what we do right now, Big Data and what it makes possible will be either a boon or a bane. Here's how to make it work for us, rather than against us.

Big Data is Essential

How we handle Big Data and what we build with it will determine how successful we are in the 21st Century.

- It is already immensely valuable, as evidenced by the valuations of the world's biggest tech companies. It will only become more so as corporations use it to train economy and society scale AI's[1].

[1] The AIs that are currently being developed aren't the human equivalent AIs of science fiction. They are closer to symbionts that live in the space between us, feeding off of the data we produce and providing services to us in return. It's useful to think of these AIs as an intelligent interface layer between us as individuals and everything else: other people, technological artifacts, our work, and the external world (increasingly as AR emerges).

- Every product and service sold will eventually utilize this data *and* these AIs. If we successfully harness the development of Big Data, it will drive economic prosperity and societal well-being well for decades to come.

- There are three major socioeconomic approaches to Big Data: China's centrally managed approach (sacrifice freedom for economic prosperity), Europe's opt-out privacy approach (sacrifice economic prosperity for traditional social stability), and the corporate-led approach used by the US and most of the world (this path is up to us).

Data Ownership

If Big Data is valuable, how do we make it work for us? We start with a critical early reform: *data ownership*.

- The closest model for our current system is feudalism. Lords/corporations own all of the data to build AIs of immense value. Corporations farm us for our data both as private citizens and while at work.

- To cast off this feudal system, we should apply the same solution that worked in the past: ownership. In the past, that meant giving people the right to own land and exercise rights over its use. In our current situation, that means giving people the right to their data and exercise rights over its use.

- Data ownership works, in practice, by allowing people to aggregate their data safely, pool it with other people's data to increase its value radically, and generate benefits (royalties, services, etc.) by licensing its use by third parties.

Digital Rights

With Big Data, we run the risk of a long night of data-fueled oppression. Here's how to avoid that future.

- Big Data and the AIs derived from it are already being used to monitor and control societal discourse (and increasingly behaviors) in real-time, down to the conversational level. Worse, these big systems can punish infractions with bans

that disconnect people from the myriad of online services that are now essential to modern life (think: disconnection as an open-air gulag).

- To avoid Big Data becoming a means of ubiquitous oppression, as we see elsewhere, we need digital rights. These rights would enumerate our freedoms. Of speech: what can't we say online in public or in private? Of association: when can you be banned, and when would algorithmic soft bans be permissible (you can publish, but nobody can see it)? Of resolution: requirements for the rapid notification of actions taken and the *resolution* of disputes.

- Big Data can create barriers to small business success. Small businesses suffer from the same problems as individuals -- from barriers to access (only the company store allows access, and it's terribly expensive) to data loss (the big data incumbents capture customer data to product mix data to customer service data and use it against the business). Therefore, we can adapt many of the remedies needed to protect individuals, to protect small businesses.

Digital Identity

To tie this all together, we need a new form of digital identity.

- Digital identity is in addition to anonymity and not a replacement for it. Digital identity will serve as a way to *dampen* the disruption we currently see online.

- Digital identity will serve as a means of exercising ownership rights over data (from claiming ownership to licensing it to collecting benefits).

- Digital identity will allow us to exercise our freedoms -- from rights of speech to rights of association to rights of speedy resolution of disputes.

The Global Guerrillas Report is a reader-supported research service that covers the intersection of warfare, technology, and politics. It is available for a modest pledge of support on Patreon: https://www.patreon.com/johnrobb

HEARING BEFORE THE UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON COMPETITION POLICY, ANTITRUST, AND CONSUMER RIGHTS

September 21, 2021

Testimony of Steve Satterfield
Vice President, Privacy and Public Policy
Facebook, Inc.

I. Introduction

Chairwoman Klobuchar, Ranking Member Lee, and members of the Subcommittee: good afternoon and thank you for the opportunity to be here today. My name is Steve Satterfield, and I am Vice President of Privacy and Public Policy at Facebook. I have been with the company for seven years. In my current role, I focus on developing and sharing Facebook's perspectives on data regulation globally.

I appreciate the Subcommittee's interest in the topics of today's hearing and the work that you all do to ensure the competitiveness of American markets. I believe Facebook has an important perspective on these issues, given the substantial contributions we have made to the technology sector in the nearly twenty years since our founding.

I also welcome the chance to engage on the topics of data and privacy. We believe that many of the concerns expressed by Congress and other stakeholders with respect to privacy issues can be addressed by appropriate legislation, and we stand ready to be a productive partner in those efforts. As we have said for some time now, we support updated rules of the road for the internet and privacy regulations that will set more consistent data protection standards that work for everyone.

Facebook provides many ways to communicate, discover, share, and connect with people, businesses, news, and entertainment. We also help millions of businesses reach and engage with their customers. To earn people's time and attention, we compete fiercely with many other services across the world.

Facebook respects the role of Congress in shaping our nation's competition policy and wants to be helpful where we can. We strongly believe that we are a force for good in the world, and I look forward to discussing our products with you. The reality, however, is that our company is currently facing multiple lawsuits, including those brought by the Federal Trade Commission and a number of state attorneys general, that limit what I will be able to address today. As we informed the Subcommittee well in advance of the hearing, the litigation process will necessarily limit the extent of my testimony. Nevertheless, we appreciate the invitation to participate in today's hearing, and I am glad to be able to share what I can.

II. Facebook Uses Data Responsibly

Like many services, Facebook helps people share, connect, communicate, or find interesting content. Each day, Americans use Facebook to connect with people, businesses, and other entities; share and view content, including videos, photos, livestreams, posts, and messages; read the news; join communities of interest; and set up fundraisers for good causes, among many other things. All of these activities support our mission to give people the power to build community and bring the world closer together, and data helps make all of them possible. We believe that our products are most useful when people can connect with what they care most about. People around the world choose to use our products not because they have to, but because they want to—because our products make their lives better.

At Facebook, we use data responsibly to provide personalized experiences. We also use information to, among other things, improve our products; provide measurement, analytics, and other business services; promote safety, integrity, and security; communicate with people who use our services; and innovate for social good, including by connecting and lifting up marginalized communities and addressing humanitarian crises. For example, Facebook's innovative use of data helps people to understand what is needed in the first hours of a disaster or the public conversation around a health crisis, information that is crucial to decision-making but previously was either unavailable or too expensive to collect in a timely manner.

Data also helps us show people better and more relevant ads, which keeps Facebook free. And it lets advertisers reach the right people, benefiting more than 10 million businesses and non-profits that use Facebook every day to advertise to those that might be interested in their product or cause. Our advertising platform can accommodate almost every budget, and we help advertisers reach their target audience and maximize their impact. Our advertising services have enabled numerous businesses to grow, create jobs, and more effectively compete, leading to more choice and better products for consumers.

We take very seriously our responsibility to protect the data people entrust us with. We also seek to ensure that the machine learning we use in processing people's data is applied in a responsible manner. We invest billions of dollars each year in people and technology to keep our platform safe, including protecting people's data. We work around the clock to help protect people's accounts, and we build security into Facebook products.

We further offer a number of tools that provide people transparency and control over the data we receive. Our approach is based on the belief that people should be able to control who can see what they share and how their data shapes their experience on Facebook. People can control the audience for their posts and manage how apps receive their data. They can choose people, Pages, Groups, and Events to connect to. They can provide feedback on posts they see on Facebook—feedback, for example, that they want to see less of a particular kind of post or fewer posts from a particular person or Page. They also have options to remove content they share from Facebook.

We have steadily made improvements to the privacy protections and controls we offer, and we continue to invest in building new privacy technology. Our goal is to be clear about how our apps work and give people control over their experience, so we've worked with policymakers, regulators, academics, civil society, businesses, and other stakeholders over the years to build tools

that show people how their information is used and let them manage it. For example, people can tap Why Am I Seeing This Ad? on ads in News Feed to get more information and control over what they see going forward. This tool shows people reasons why they're seeing a certain ad, whether it's based on interests that matched them with the ad or actions they took on the business' website; and, where possible, people can see how that information was gathered. From there, people also have easy access to controls, like Ad Preferences, which lets them manage the ads they see, learn more about how ads work, and hide ads from specific advertisers or topics. And our controls aren't just for ads. We also offer tools like Manage Activity and Privacy Checkup so people can easily customize their overall experience on Facebook based on what's right for them. Millions of people use our Privacy Checkup tool each month.

We also offer a variety of tools to help users understand the data Facebook has about them. This includes the Access Your Information tool, which allows users to see information such as their recent activity, security and recent login information, advertisers they've interacted with, and more. And to provide more transparency and control around these practices, we have rolled out a way for people to manage their off-Facebook activity. Off-Facebook Activity lets people see a summary of apps and websites that send us information about their activity and allows them to disconnect this information from their account if they want.

At Facebook, we believe that if people share data with one service, they should be able to move it to another. Making it easy to move data to new services unlocks exciting opportunities. This is why we offer the Download Your Information tool, enabling people to download a copy of the information they share on Facebook in a format that is easy to view, or a machine readable format, which could allow another service to import it. Additionally, we participate in the Data Transfer Project, a collaborative effort with Apple, Google, Microsoft, SmugMug, and Twitter to build a common way for people to transfer this data between online services. The goal of this project has been to make it easier for users of services of any size to securely and directly transfer data from one service to another. Building on the Data Transfer Project's open-source framework, in 2020, we launched the Transfer Your Information tool. We continue to build out the capabilities of this tool, and today it enables users to directly transfer their Facebook photos, videos, posts, notes, and events to a variety of relevant destinations that include WordPress, Blogger, Google Docs, Google Photos, Google Calendar, BackBlaze, Dropbox, Photobucket, and Koofr. We want to build practical portability solutions that can enhance participation across the digital ecosystem, and we continue to invest in adding new capabilities to strengthen our data portability offerings.

Of course, there are always risks when people transfer data online. Congress should set out clear rules on data portability so that we can continue to scale the tools we've built to better enable people to safely and securely move their data between services. Along the same lines, Congress could also create rules to govern how platforms should use, analyze, and share data for the public good.

We store the information that we receive in multiple data centers throughout the country and the world, and we strive to make these facilities climate-friendly. In fact, in 2011, Facebook was one of the first companies to commit to supporting its facilities with 100% renewable energy. Today, the company's U.S. data center fleet is supported by 100% renewable energy, and Facebook is on track to maintain this commitment for future data center developments and expansions.

Finally, it is important to note that our data analysis facilitates cooperation with law enforcement as they seek to protect us all. We have a long history of working successfully with the Department of Justice, the FBI, state and local law enforcement, and other government agencies around the world to address a wide variety of threats to our platform. We reach out to law enforcement when we see a credible threat of imminent harm. We contact federal, state, or local law enforcement depending on the specific circumstances of a threat. We also have robust processes in place to handle government requests we receive, and we disclose data in accordance with our terms of service and applicable law.

III. Facebook Innovates Constantly

We work constantly to improve our services and products, including by introducing fresh features and developing new ways for people and businesses to connect. Data is part of that effort.

When Facebook was first created, the site consisted primarily of text details about each user. Today, we offer a much wider variety of capabilities through the Facebook family of products and services. Facebook users can create new content, read news, broadcast or watch live video, play games, connect with businesses, buy and sell their own products, send and receive payments, organize groups and events, and raise money for important causes, among many other options. Like many services, WhatsApp provides free, secure communication, including voice and video calls. Instagram offers world-class tools to create and share content based not just on photos, but also videos, augmented reality, and more.

Providing the highest-quality features and best experience for consumers is at the heart of what we do. We offer innovative services that people use to connect and share with their friends, families, businesses, and wider communities. Our products also allow content creators to share their creativity and build community, entrepreneurs to grow their businesses, and non-profits to hit their fundraising goals, among other things.

When Facebook launched in 2004, it had no Photos, Like button, News Feed, Messenger, Events, Shops, or Rooms. As the ways people connect and share evolved over the years alongside rapid innovations in technology, we built new and better apps and services. In turn, many of the iconic features we pioneered have been adopted and improved upon by other companies. And the Facebook family today goes beyond software, with hardware products like Oculus and Portal.

We are always working to develop technologies that enhance the way people connect and communicate, and data is key to that work. We use the data that people entrust to us to pursue new products and features that people want, and we do so because we know that if we don't constantly keep innovating and improving, we will fall behind. When Facebook started, we faced established competitors—including AOL and MySpace—with lots of user data. That did not protect them from others building better products, as success comes from creating products users value and enjoy, not from how much data you have. Apps often rise from nothing to prominence very quickly.

IV. Facebook Competes Vigorously

Facebook as we know it today would not have been possible without laws that encourage competition and innovation. We've been successful because we've made risky bets, invested, innovated, and delivered value to people, advertisers, and shareholders. As the internet has grown over the last 25 years, the ways in which people share and communicate have exploded thanks to dynamic competition. The most successful platforms mature and adapt to people's changing preferences. Our products became popular for this very reason—we constantly evolve, innovate, and invest in better experiences for people against world-class competitors like Apple, Google, Twitter, Snap, Amazon, TikTok, Microsoft, and many more. We innovate and improve constantly because we have to in order to stay relevant.

As our CEO Mark Zuckerberg has explained, we believe that strong and consistent competition is vital because it ensures that the playing field is level for all. Facebook competes hard, because we're up against other smart and innovative companies. We know that our future success is not guaranteed, especially in a global tech industry defined by rapid innovation and change. The history of technology is often the history of failure, and even industry-leading tech companies fail if they don't stay competitive, hence our focus on delivering better services for people and businesses and competing as vigorously as we can within the rules.

We face robust competition in every aspect of our business, and we only succeed when we build things that people find valuable. Today, people have more choices at their fingertips than ever before. Near-constant technological innovation has created an ever-more competitive environment, and we invest heavily in our products and services to stay relevant and competitive, committing more than $18 billion to research and development last year.

And just as people choose to use Facebook, so too do millions of businesses—large and small—choose to use our free tools and advertising products. We compete for advertising dollars with other digital platforms, from Google to TikTok, and with other channels such as television, radio, and print. Businesses choose us because our apps and services deliver real value. We are proud of our record, and we will continue to focus on building and updating our products to give people the best experiences possible.

V. Conclusion

Facebook's success rests on our ability to bring value to people's lives, and that requires us to innovate constantly. In doing so, we responsibly use and analyze data to enhance user experiences and improve our products and services that allow people to connect and share what matters most to them, recognizing that if we don't keep improving, our many competitors will, and we will lose our users and advertisers. Thank you, and I look forward to your questions.

Testimony of
Charlotte Slaiman[1]
Competition Policy Director
Public Knowledge

Before the
United States Senate
Committee on the Judiciary

Subcommittee on
Competition Policy, Antitrust, and Consumer Rights

Hearing On:
Big Data, Big Questions: Implications for Competition and Consumers

Washington, D.C.
September 21, 2021

[1] I want to thank Alex Petros, Policy Counsel, for his support in preparing this statement

Chairwoman Klobuchar and Ranking Member Lee:

Thank you for the opportunity to testify today on behalf of Public Knowledge, a nonprofit working in the public interest for over 20 years. I'm Charlotte Slaiman, a former antitrust enforcer at the Federal Trade Commission and now Competition Policy Director for Public Knowledge. We fight for an open internet, free expression, and access to affordable communications tools for everyone. Achieving these goals is only possible through robust online competition free from the control of today's digital gatekeepers. This hearing smartly zeroes in on one of the key components of this power: data. Although Big Data is most often discussed in policy circles for its privacy implications, I am very pleased that this Subcommittee is focusing on Big Data in the context of antitrust and competition policy.

Data is everything to a platform. It is the lifeblood, the currency, and the fuel that drives Big Tech and many of the products they offer. Perhaps most importantly, data is a key component that platforms use to maintain their gatekeeper power. This should be a dynamic industry where innovation can flourish, but because of the hands-off approach policymakers have taken in the past, new disruptive innovators have not had a fair shot. This hearing marks an important step toward addressing that power, and until we do so, Big Tech will continue picking winners and losers in digital markets.

Data & Gatekeeper Power

Gatekeeper power is at the root of the competition problems Big Tech presents. Expert economists and antitrust professors, policymakers here in the U.S. and abroad, and advocates the world over have identified gatekeeper power—sometimes "bottleneck power," or "strategic market status"—as the power that dominant digital platforms have over other businesses' ability to reach their customers.[2] As a result, these dominant digital gatekeepers also serve as the primary access point for key consumer data. These gatekeepers get to determine who can play the game in which they also compete. They have the incentive and ability to pick themselves as the winners of this game and pick potential competitive threats as the losers. These same gatekeepers can wield their superior access to data as a cudgel to ensure their gates remain closed—and they stay on top. We can't expect gatekeepers to give up their power just because it's the right thing to do. We need Congress to act to break open the gates and promote a competitive market.

[2] George J. Stigler Center for the Study of the Economy and the State, Committee for the Study of Digital Platforms Market Structure and Antitrust Subcommittee Report ["Stigler Report"] 32 (Jul. 1, 2019), https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf; Digital Competition Expert Panel, *Unlocking digital competition* 59 (Mar. 13, 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.

Digital gatekeepers benefit from a triumvirate of market characteristics—network effects, economies of scope and scale, and the ability to control the choice architecture that influences user behavior.[3] We see network effects when users naturally flock to the most popular services as their utility from a service is directly related to how many other people use it. The fact that most of your friends are on Facebook's social network is probably what convinced you to join Facebook in the first place and what keeps you there now. The inherent economies of scope and scale in Big Tech's products also turbocharge gatekeeper growth. It can be difficult for new platforms to compete with dominant ones, yet once a new platform gets going, each additional user results in negligible costs for the platform and exponential benefits in terms of additional data. Finally, gatekeepers have complete control over the user interface—what users see when they access the platform—and can use that interface to push them towards certain choices.

Big Data Fuels Anticompetitive Discrimination

The user interface of a digital gatekeeper has a much bigger impact than the interface of an average website or the layout of a physical store. Dominant digital platforms can pick winners and losers in the digital economy by prominently ranking someone at the top of a page or hiding someone's listing away after lots of scrolling. There are many other tools at their disposal, too. For example, some Google search results get to take up a lot of "real estate" on the search engine results page. These results can have images, bold type, or multiple clickable links to different parts of a website to really grab the user's attention. A user is much more likely to click on one of those results than one that's given fewer engaging features. Amazon chooses which retailer wins the coveted Buy Box (the "Buy Now" button that most users click on to actually buy a product), but Amazon also leverages clever site design to make it seem like the Buy Box is the *only* way for a customer to buy a particular product.[4] Most users don't even realize there are other sellers offering the same product due to this design feature.

How these design choices influence user decisions is called the "choice architecture."[5] It can be extremely effective and misused to trick customers, a phenomenon researchers have termed "dark patterns."[6] To understand and use these tools of discrimination to their greatest effect, the platforms are constantly running tests on us, the users. Based on what I click or don't click, dominant digital platforms can refine what they're doing to more accurately get the next person to click. This applies to influencing me to stay on Facebook longer, or to purchase a particular product on Amazon. Dominant platforms meticulously optimize their user interfaces to push us

---

[3] *See supra* Stigler Report, 7–8.
[4] *See* Amazon Seller Central, *How the Buy Box Works*, https://sellercentral.amazon.sg/gp/help/external/help.html?itemID=37911&ref=efph_37911_cont_home
[5] Richard H. Thaler et al., *Choice Architecture*, SSRN (Apr. 2, 2010), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1583509.
[6] Sara Morrison, *Dark patterns, the tricks websites use to make you say yes, explained*, Vox (Apr. 1, 2021), https://www.vox.com/recode/22351108/dark-patterns-ui-web-design-privacy.

to behave in a platform's best interest. This could mean keeping us constantly engaged with a product or it might mean keeping us *away from* companies that could challenge gatekeeper dominance if they were given a fair shot on the platform.

The platforms also can choose winners and losers through the Big Data-driven algorithms they develop and use to determine which options they'll show to a user. Users may be harmed by the high degree of tracking and engagement needed to target these offerings.[7] They may also be harmed by seeing fewer options and by the assumptions the algorithm makes about us. What a platform's algorithm thinks you'll click on isn't always what's best. We as users could lose out on products we might actually want if our full range of short-term and long-term interests aren't adequately captured by these blunt algorithms. Platforms also offer behavioral targeting for use in perpetuating racial and gender discrimination. Federal enforcers have accused Facebook of targeting housing ads based on race, in violation of the Fair Housing Act.[8] Prospective employers can target their job ads at young men, leaving qualified older workers and women out in the cold.[9]

And this doesn't just harm users. Businesses trying to reach us through Google or Facebook will also suffer if they don't fit into the prescribed categories that the platforms expect based on the Big Data algorithms they deploy. If I haven't previously consumed much content from creators of color, Google and Facebook probably aren't going to show that to me.[10] If I haven't previously purchased foods Amazon deems "ethnic" they're probably not going to highlight those for me. Businesses assessed by the platforms to not be appealing to large groups of customers or to wealthy customers may be denied a chance at fair competition. If a grocery store declines to put a product on their shelves, that producer can go elsewhere. If Google decides your product won't be popular with the people in your city who can afford it, your business would be in much bigger trouble.

Even seemingly minor changes to these algorithms can have disastrous effects for small businesses. Facebook's infamous "pivot to video" was one such case.[11] Facebook determined that videos were getting more attention on their site, and started promoting video content much

---

[7] For an excellent review of the collateral damage to everyday life caused by this complex advertising ecosystem, *see* TIM WU, THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE (2016).
[8] Katie Paul, *U.S. Charges Facebook with racial discrimination in targeted housing ads*, REUTERS (Mar. 28, 2019), https://www.reuters.com/article/us-facebook-advertisers/u-s-charges-facebook-with-racial-discrimination-in-targeted-housing-ads-idUSKCN1R91E8.
[9] Ava Kofman & Ariana Tobin, *Facebook Ads Can Still Discriminate Against Women and Older Workers, Despite a Civil Rights Settlement*, PROPUBLICA (Dec. 13, 2019), https://www.propublica.org/article/facebook-ads-can-still-discriminate-against-women-and-older-workers-despite-a-civil-rights-settlement.
[10] *See* Chris Lewis, *Fighting the Free Speech Divide Requires Interoperability and Privacy Protection*, TECHDIRT (May 29, 2020), https://www.techdirt.com/articles/20200527/11104344587/fighting-free-speech-digital-divide-requires-interoperability-privacy-protection.shtml
[11] Will Oremus, *The big lie behind the "pivot to video,"* SLATE (Oct. 18, 2018), https://slate.com/technology/2018/10/facebook-online-video-pivot-metrics-false.html.

higher than other types. Whole industries had to change their business models to keep up. In the news industry in particular, many writers were laid off to make room for hiring new video content teams.[12] Later, we found out that Facebook had misled advertisers and publishers. Video posts on Facebook actually were not receiving nearly the attention Facebook had claimed. Google's search algorithm has its own esoteric preferences it thinks users prefer, like recipe blogs that have a cute (or annoying) little story you have to scroll through before you get to the actual recipe. This influences what small businesses do to "work the algorithm" to access users through the dominant platforms' gates.

Wielding Data Access as an Anticompetitive Weapon

Dominant platforms have strategically positioned themselves at internet bottlenecks. Many times, companies are forced to pay gatekeeper tolls to access customers and data. These tolls can take the form of monetary payments and/or unfair data sharing and access conditions that reinforce the platform data advantage. The penalties for not towing the gatekeeper line can end once-promising products or services.

For example, access to the Facebook network is a lifeline for upstart social networks. The strategic cutting off of that access for potential rivals is a pillar of the ongoing Federal Trade Commission's case against Facebook.[13] According to the FTC, Facebook retooled its network access as an "anticompetitive weapon"—only granting access to companies that agreed not to compete with Facebook or support its rivals. Potential competitive threats were cut off as they began to exhibit growth that could threaten Facebook. Soon after losing access to the Facebook network, these would-be rivals promptly folded, depriving consumers of services they otherwise might have enjoyed.

Finding out who is collecting your data is not as simple as the brand you see at the top of the page. You might be surprised to learn that it's actually Google and Facebook collecting your data instead. If you use Google to find a news article, you may end up not on the newspaper's website, but one of Google's Accelerated Mobile Pages (AMP). In that case, it's actually Google that gets to track my data, and if the newspaper wants to know which of their articles is getting the most readers, they need Google to "share" that data with them.[14]

---

[12]Alexis C. Madrigal & Robinson Meyer, *How Facebook's Chaotic Push Into Video Cost Hundreds of Journalists Their Jobs*, THE ATLANTIC (Oct. 18, 2018), https://www.theatlantic.com/technology/archive/2018/10/facebook-driven-video-push-may-have-cost-483-journalists-their-jobs/573403/.
[13] Amended Complaint, Fed. Trade Comm'n v. Facebook, Inc., No: 1:20-cv-03590-JEB (D.D.C. Aug. 19, 2021).
[14] Competition & Mkts Auth., Online Platforms and Digital Advertising: Market Study Interim Report (2019) ¶ 5:252 ("Publishers... have concerns around restrictions on their ability to monetise these pages and their ability to access data generated from consumers' interaction with them.").

In order to advertise to you, a lot of companies use third party cookies to track your web browsing activity. But most browsers have begun blocking third party cookies or have announced they will block third party cookies—including Google's Chrome browser. Some browsers, like Brave and Firefox, have taken the position that they will never enable passive tracking of their users. Google has not; they have implemented their "privacy sandbox" as an alternative to cookies. Now instead of third-party cookies doing the tracking, it's your web browser that is tracking you. Under their new system, Google has even more control over your personal data, because it is increasingly one of the only options for tracking people across the web. Third party cookies were bad for privacy. However, this new system from Google doesn't prevent tracking from occurring; but for many users it means Google is the only one able to do the tracking.[15]

As a user, I don't want to rely on Google's or Facebook's interpretations of privacy. We need comprehensive federal privacy legislation that protects users from Google's and Facebook's data collection and use just as much as it protects us from other companies.

Big Data is a Major Incumbency Advantage

Digital gatekeeper platforms also exhibit increasing returns to scope and scale, largely because of how the value of data increases so significantly when it's merged with other data. Twice as much data isn't just twice as good for a company, but many times more so. This is true both on an individual and a group level. A company that is able to aggregate multiple sources of data on you will be much more powerful than one that is relegated to a single or few sources.[16] Think of a user fully integrated into the Google ecosystem. Google knows where you are by looking at your Android phone or your Google Maps app. They know what videos and shows you like from YouTube and YouTube TV activity. They know your interests from your Chrome web browsing and Google search history. All of this data can be merged together to build an in-depth profile about you and what you might be interested in right now. A company with just one of those sources of data can't predict your behavior as accurately.

Data from large groups of individuals is similarly more and more valuable with each new user added. Data about other users can fill in the few things a company doesn't know about you by looking at people who are similar to you on the data points they do have. If other white women my age who live in my neighborhood, work in Dupont Circle, and follow Epic Gardening on

---

[15] *See* Cory Doctorow, *Fighting FLoC and Fighting Monopoly Are Fully Compatible*, ELECTRONIC FRONTIER FOUNDATION (Apr. 21, 2021), https://www.eff.org/deeplinks/2021/04/fighting-floc-and-fighting-monopoly-are-fully-compatible; Charlotte Slaiman, *Data Protection is About Power, Not Just Privacy*, PUBLIC KNOWLEDGE (Mar. 3, 2020), https://www.publicknowledge.org/blog/data-protection-is-about-power-not-just-privacy/.

[16] Tom Wheeler, *Big tech and antitrust: pay attention to the math behind the curtain*, BROOKINGS INSTITUTE (July 31, 2020), https://www.brookings.edu/blog/techtank/2020/07/31/big-tech-and-antitrust-pay-attention-to-the-math-behind-the-curtain/.

Instagram like something, Big Data analyzers can assume I will like it, too. Combining a variety of data points helps to more effectively influence users and discriminate between them.

The dominant platforms sometimes argue that data ages rapidly, so a new competitor could quickly amass the data needed to compete. This is theoretically true, but it is not just old data that today's dominant digital platforms control. Users are still today locked in to these platforms through their gatekeeper power, so the platforms continue to have access to ongoing data streams. These data streams can be used to continuously update algorithms to stay on top. They can also keep platforms updated about the users so as not to rely on just static or past data about them. This allows platforms to not just "know" their users, but see how their users change over time—often in response to the algorithms that platforms created using older user data. This cycle of collection, use, and iteration gives platforms significant power over their users.[17]

By taking advantage of the significant increase in the value of a data stream when it's merged with other data streams, vertically integrated and conglomerate firms like the dominant digital platforms can exacerbate barriers to competition. The wide variety of products Google offers gives an illustrative example. Google can see from my calendar and my email that I have a meeting coming up across town. Using Google Maps, it can tell me exactly when I should leave for said meeting. There are competitors that offer different navigation apps, calendars or email clients, but it's very difficult for a smaller company to offer all three. Simultaneously entering multiple markets to compete with multiple arms of the Google leviathan at once is called dual-market entry, a notoriously difficult feat according to antitrust economists.[18] Consumers could lose out on a better single product if innovative entrepreneurs are blocked from the market unless they can debut multiple great apps at the same time. This huge entry barrier is one way that vertical integration and conglomeration results in less competition against Big Tech and fewer options for consumers.

Finally, gatekeepers can prevent rivals from getting the data they need to effectively compete. This is perhaps best seen in the infamous episode of Google starving Bing of data it needed to effectively challenge its market power in online search.[19]

Solutions

---

[17] *See, e.g.*, Will Oremus, *Facebook keeps researching its own harms — and burying the findings*, THE WASHINGTON POST (Sept. 16, 2021), https://www.washingtonpost.com/technology/2021/09/16/facebook-files-internal-research-harms/.

[18] *See, e.g.*, U.S. Dept. of Justice & Fed Trade Comm'n, Vertical Merger Guidelines 7–8 (2020), https://www.ftc.gov/system/files/documents/reports/us-department-justice-federal-trade-commission-vertical-merger-guidelines/vertical_merger_guidelines_6-30-20.pdf.

[19] *See* CMA Report, *supra* note 13, at ¶ 24; Fiona Scott Morton & David Dinielli, Roadmap for a Monopolization Case Against Google Regarding the Search Market 37, OMIDYAR PROJECT (June 2020), https://omidyar.com/wp-content/uploads/2020/09/Roadmap-for-a-Monopolization-Case-Against-Google-Regarding-the-Search-Market.pdf.

Competition is not a panacea for the challenges of Big Data. We also urgently need new privacy laws to protect users, as well as a digital regulator to comprehensively address the policy questions surrounding digital platforms. We can't afford a race to the bottom on privacy with companies scrambling to maximally exploit consumer data. It's not the realm of antitrust or competition policy to decide what markets are just too harmful to people and, thus, not worth having at all. A comprehensive federal privacy law can be pro-competitive by creating a level playing field for dominant incumbents and new entrants alike.

At the same time, we need new laws and rules focused on promoting fair competition on and against dominant gatekeeper platforms to give back some real control to consumers and business users. Until we have a real choice to leave these platforms if we're not happy with them, they won't care about doing what is in their users'—our—best interest. Thankfully, there's already a template for legislative change that could have a major impact on the power of Big Tech and Big Data. The package of antitrust bills focusing on Big Tech that recently passed through markup in the House Judiciary Committee represents a key piece of the solution, as does broad antitrust reform as Chairwoman Klobuchar has proposed here in the Senate. The recently introduced *Open App Markets Act* from Senators Blumenthal and Blackburn is also an important part of the reform solution. These solutions aren't mutually exclusive. Both sector-specific and economy-wide antitrust reforms are needed. I hope that we will see Senate companions to the House legislation, and a House companion to the Senate legislation.

Interoperability, Data Portability, and Delegatability

Interoperability, data portability, and delegatability are the privacy-protective ways to neutralize the power that Big Data confers upon dominant digital platforms. Right now, if I'm frustrated with how Facebook treats my data, I don't really have the option to leave because my friends and family, the businesses, groups, and even schools I need to communicate with are on Facebook. Facebook is able to rest on its laurels and faces little incentive to innovate or actually protect my privacy. When the Stop Hate for Profit campaign last year convinced many advertisers and users to boycott Facebook because of their refusal to moderate hateful content on the platform, Mark Zuckerberg said he wasn't concerned, that they'll be back "soon enough."[20] He knows that other platforms can't compete because his network is so much larger. Interoperability would address these network effects and allow competition to flourish by letting users connect back to Facebook from a new competitor if they choose.

Data portability allows users to bring their data with them from a dominant platform to a competitor. For users, this helps address one of the high switching costs in leaving a platform. Think about how much time you've spent building out your social media presence—all the

[20] James Clayton, *Zuckerberg: Advertisers will be back to Facebook 'soon enough,'* BBC (July 2, 2020), https://www.bbc.com/news/technology-53262860.

uploaded photos, comments, statuses, etc. If the only way to end your relationship with Facebook is to lose all this data, you may be wary about leaving. Portability also helps upstart competitors because when a customer chooses them over the incumbent, the new platform gets not just a new user and the data they choose to share going forward, but also the past data they choose to port over from the incumbent. That should make dominant platforms fight harder to win your business and give new entrants more of a leg up. To be clear, data portability on its own will not be sufficient to jumpstart competition.

Delegatability allows users to designate a third party to manage their online interactions and account settings (including privacy settings) across multiple platforms. If interoperability and portability work as intended, we expect to see new entrants actually competing against some of these dominant platforms. Delegated services can simplify the process of interoperability across multiple platforms and help consumers receive the maximum benefit from it.

Thankfully, we have an excellent congressional blueprint in the form of the *ACCESS Act*, a bipartisan and bicameral bill with origins on this Subcommittee. What I love about the *ACCESS Act* is that it puts users in control and puts privacy first. If a user wants to move their data elsewhere or try out a new competitor they can. And the Act explicitly lays out detailed privacy protections such as giving the FTC explicit rulemaking authority over the privacy of relevant data, specifying that any data gleaned cannot be commercialized, and creating data minimization requirements. The *ACCESS Act* is an excellent example of a bill that couples massive benefits for both privacy and competition and should be passed as soon as possible.

Non-Discrimination

These platforms can abuse their gatekeeper power to freeze out would-be competitors from the market and one of the tools for that discrimination is Big Data. Gatekeeper platforms can put their own products first on the page, give them the best attention-grabbing design, and point users away from companies that might threaten their gatekeeper power. They can give their own services unfettered access to consumer data that they zealously guard from others. They can even misuse competitor data (data that the competitor must give as a condition of competing on the platform) to launch rival products or hamstring competitors.[21] While this offends our basic notions of fairness, without greater legislation and regulation this behavior would be very difficult to stop using our existing antitrust laws.

A non-discrimination law like House Antitrust Subcommittee Chairman David Cicilline's *American Choice and Innovation Online Act* could help solve these tough problems. Dominant

[21] *See* Makena Kelly, *Jeff Bezos can't promise Amazon employees don't access independent seller data*, THE VERGE (July 29, 2020), https://www.theverge.com/2020/7/29/21347083/jeff-bezos-amazon-tech-antitrust-hearing-jayapal-questioning.

platforms would be prohibited from advantaging their own products and services or disadvantaging the products and services of their rivals or potential competitors. There are also specific prohibitions on using non-public data from a platform's business user to compete against them and impeding or restricting the portability or interoperability of business user data. The proposed law was written with data issues in mind and would target some of the most pernicious platform behaviors.

Merger Limitations

Today's Big Tech titans did not always grow organically, but through strategic acquisitions to fend off rivals and maintain their hold on their respective markets. Many times, a platform will acquire a company to integrate their data or data streams with the treasure trove of data the platform has already accumulated or data streams they already have access to. This feeds into the increasing returns to scope and scale that help entrench Big Tech market dominance. Efforts by advocates and enforcers to block or unwind these deals have been an uphill battle. We need our laws to better recognize the power that can come from conglomerating sources of data that may at first seem unrelated. Bills like Rep. Jeffries' *Platform Competition and Opportunity Act* would represent an important step forward. It would chill predatory acquisitions by dominant tech platforms and allow innovation and competition to flourish. Chairwoman Klobuchar's *Competition and Antitrust Law Enforcement Reform Act of 2021* would also be a great help in this area. Amending the Clayton Act merger standard to ban mergers that "create an appreciable risk of materially lessening competition" and shifting the burden to the merging parties in certain instances would both help our overworked enforcers and stop the worst anticompetitive mergers from moving forward.

Structural Separation

Merging multiple data sources helps huge conglomerates know even more about us, so they can even more effectively manipulate and discriminate against us. It's important that antitrust enforcers have the ability to sue dominant digital platforms collecting data across multiple lines of business to separate off a line of business that's posing a conflict of interest. Rep. Jayapal's *Ending Platform Monopolies Act* would provide this needed tool to antitrust enforcers and sets forth the situations in which it can be used.

App Market Reforms

The *Open App Markets Act* is targeted at the worst abuses of dominant app stores, a notorious and narrow internet bottleneck. The bill would allow apps to use alternative payment systems and require the app store operator to give third parties fair access to device and software features. There is also a specific ban on using non-public data gleaned from an app to compete against the

app. The bill requires operating systems to offer interoperability, including letting users choose third-party apps as defaults and use alternative app stores.

Broad Antitrust Reform

Purposeful narrowing of our antitrust laws by the courts have left big business with license to engage in a host of anticompetitive conduct. A myopic focus on price and other easily quantifiable effects leaves out important innovation and consumer choice harms that antitrust is supposed to address. It's well past time for our antitrust laws to receive a refresh. The Chairwoman's *Competition and Antitrust Law Enforcement Reform Act of 2021* would help rein in the power of Big Data by updating the legal standards for blocking mergers and stopping exclusionary conduct. The bill also restores an appropriate definition of market power that goes beyond prices. Antitrust enforcers can bring in anticompetitive data practices as direct evidence of market power. The newly proposed Division of Market Analysis could also study data markets to improve enforcement.

Conclusion

For decades now, Washington has taken the perspective that we need to let digital businesses run wild to see what great innovations they might come up with. But today, unscrupulous data practices and consolidated power have led us to a place that isn't anyone's dream of what the internet was supposed to be. These largely unregulated platforms have been allowed to amass powerful gatekeeper roles in multiple markets, where they need not fear competition or government intervention. For users to really have control, we need to have a *real* choice to leave these platforms. We need real competitors and we need switching to be easy. To get those things, we need new laws and rules to promote fair competition on and against gatekeeper platforms like Google and Facebook. Congress has already done laudable work of introducing a series of bills to combat these harms. The best time to pass them was 10 years ago. The second-best time is now.

Senator Blackburn
Questions for the Record to Sheila Colclasure
Global Chief Digital Responsibility & Public Policy Officer, IPG Kinesso

1. It's imperative for the U.S. to get a national consumer privacy law in place—the EU and China have already done so. Given consumer concerns about how their data is being used online, what should that regime look like? What are obstacles the United States faces in getting to that point?

Senator Chuck E. Grassley

Question for Ms. Sheila Colclasure:

1. There is debate over whether Big Data should be regulated through the lens of consumer protection and privacy or whether antitrust laws should be used to address competition concerns with the collection of data. Do you have an opinion about the best approach to address this issue or should we be looking at a combination of different approaches?

JON OSSOFF

U.S. SENATOR FROM GEORGIA

QFRs for Sheila Colclasure

Global Chief Digital Responsibility and Public Policy Officer, Kinesso

September 28, 2021

Judiciary Committee
Subcommittee on Competition, Antitrust, and Consumer Rights
"Big Data, Big Questions: Implications for Competition and Consumers"
Hearing held on September 21, 2021

1) Please list any instance where any IPG company provides or has ever provided products or services to ***any*** federal agency, or to any federal prime contractor or federal subcontractor for purposes of supporting a Federal program, including the nature and value of the products or services provided. As part of this response, please describe the nature of Acxiom's 2019 contract with the United States Special Operations Command, including how Acxiom supports "Project Red Mouse." If necessary, submit a classified annex to the Committee on the Judiciary to ensure this information responsive to this question is complete.

2) Please list any instance where any IPG company provides or has ever provided products or services to any state or local law enforcement agency.

3) Please list all bids for federal contracts submitted by any IPG company, even if such bids were unsuccessful. Specify the federal agency, the title and purpose of the bid, the products or services that were to be provided, and where applicable the estimated or suggested value of the contract(s).

4) Please list all bids for contracts with state or local law enforcement agencies submitted by any IPG company, even if such bids were unsuccessful. Specify the agency, the title and purpose of the bid, the products or services that were to be provided, and where applicable the estimated or suggested value of the contract(s).

5) Please describe any instance where any IPG company provides any product or service to any foreign governmental entity, foreign state-owned enterprise, or foreign political entity (e.g. foreign political parties, political candidates, or political campaigns).

6) Please describe any instance where any IPG company provides or has provided any product or service to any foreign or U.S. business for purposes of supporting that business' contract work on behalf of any foreign governmental entity.

7) Please describe any relationship through which any IPG company receives personally identifiable data or any data pertaining to U.S. persons from federal, state, or local governments or government agencies. As part of this response, please describe whether data received includes information about the online presence of individuals, such as social media accounts.

8) Please describe in detail the sources from which Acxiom or other IPG companies obtain unique device identifiers, including IMEI, IMSI, MAC addresses, or IDFA/Ad-IDs.

   a. If you receive or obtain unique identifiers from commercial partners, please describe the means by which those partners obtained the identifiers.

9) Please describe efforts by any IPG company to link unique device identifiers with the IP addresses of residential or commercial internet connections.

10) Please describe any products or services any IPG company offers to clients to enable them to see connections between personally identifiable data, such as SSN, home address, email address, or telephone number, and sensitive data, such as web browsing activity, web search history, or purchase history.

11) Please describe any contractual limitations Acxiom places on entities' use or disclosure of data about individuals.

   a. Does Acxiom monitor its clients for contract adherence? If so, how?

   b. Has Acxiom or any other IPG company discovered or become aware of a contracting partner's contractual breach relating to personally identifiable information? If so, please describe any resulting actions taken by IPG or an IPG company.

12) Other than its website, what steps does Acxiom take to alert consumers to their ability to opt out of the company's use of their data?

   a. Do you treat opt-out requests from California residents differently than opt-out requests from residents of other states?

   b. If so, please describe any differences in how Acxiom would treat data about a person from California after receiving an opt-out request, compared to how it would treat data about a person from another state who submitted an opt-out request.

Senator Tillis Questions for the Record – Big Data, Big Questions: Implications for Competition and Consumers

Sheila Colclasure, Global Chief Digital Responsibility and Public Policy Officer, IPG Kinesso

1. The term "data" can have multiple meanings, which can sometimes generate confusion in policy discussions. How would you define "data" and "big data", as used in your written testimony?
    a. How would you define consumer and user data, specifically what would be included and excluded from these definitions?
    b. Would this include user uploaded videos, images, and text?
    c. Would such content be considered part of the "user" data, even if it includes content that originates from other sources?
    d. Does it include data in which intellectual property rights, including copyright, trade secret, trademark, or design rights, may subsist?
2. Your testimony advocates for an expansive view of competition law that would account for the flexibility to account for data-related issues., and advocates for the Committee to consider privacy and competition to be interrelated.
    a. Would the same consideration be extended to other "big data" issues, such as intellectual property rights, cybersecurity, national security, data protection, and other issues?
    b. How should antitrust law be tailored to appropriately account for privacy rights, or other legitimate concerns such as intellectual property rights?

3. Ms. Slaiman advocates for "a digital regulator to comprehensively the policy questions surrounding digital platforms."
    a. Do you agree that this is necessary?
    b. Given the many issues beyond privacy and competition that address and implicate digital policy—including cybersecurity, national security, consumer rights, free speech, and intellectual property concerns—what existing agency would be the best situated, in your view, to carry out this role?
    c. Is it important to you that the regulator should be politically accountable?

Senator Chuck E. Grassley

Questions for Mr. Markham Erickson:

1. Google monetize user's data by selling targeted advertisements. In the second quarter of 2021 Google had advertising revenues of $50.44 billion. How much is the average American's data worth to Google?
2. There is debate over whether Big Data should be regulated through the lens of consumer protection and privacy or whether antitrust laws should be used to address competition concerns with the collection of data. Do you have an opinion about the best approach to address this issue or should we be looking at a combination of different approaches?

Senator Josh Hawley
Questions for the Record

Markham Erickson
Vice President (Government Affairs and Public Policy), Google

1. **Please provide copies of all research findings or reports, whitepapers, slideshows, meeting recordings, or other documentation circulated within Google, over the past ten years, pertaining to each of the following topic areas:**

   a) **Addiction or addictive behaviors associated with the use of Google's products and services;**
   b) **Depression and/or self-harm associated with the use of Google's products and services;**
   c) **Impact of Google's products and services on the mental health and wellness of users under age 18;**
   d) **Extent to which Google's products and services are accessed by users under age 13;**
   e) **Development of novel products or services targeted specifically to users under age 13.**

2. **Please provide the following information:**

   a) **How much revenue, in the aggregate, does Google estimate that it makes from users under 18?**
   b) **How much revenue does Google estimate that it makes from *each individual* user under 18?**
   c) **How much revenue, in the aggregate, does Google estimate that it makes from users under 13?**
   d) **How much revenue does Google estimate that it makes from *each individual* user under 13?**

3. **Has Google ever required a third party to alter search results, provide internal data, or make other nonmonetary contractual concessions in order to distribute or otherwise obtain access to Google's apps, including YouTube and YouTube TV?**

Senator Tillis Questions for the Record – Big Data, Big Questions: Implications for Competition and Consumers

Markham Erickson, Vice President, Government Affairs & Public Policy, Google

1. The term "data" can have multiple meanings, which can sometimes generate confusion in policy discussions. For example you refer to the publicly available web as an important data set. How would you define "data" and "big data", as used in your written testimony?

    a. How would you define consumer and user data, specifically what would be included and excluded from these definitions? For example, the section of data portability refers to the ability of users to export "their data".

    b. Would this include user uploaded videos, images, and text?

    c. Would such content be considered part of the "user" data, even if it includes content that originates from other sources?

    d. Does it include data in which intellectual property rights, including copyright, trade secret, trademark, or design rights, may subsist?

2. Ad-revenue used to support online piracy is a longstanding problem. Criminals profit by receiving advertising dollars in exchange for giving users free access to stolen movies, music, books, software, and other materials—stealing money from hardworking creators, including many small businesses and individual artists. A recent report found that over *a billion dollars a year* in advertising goes to supporting online pirated content.[1] Both the US and EU have been working on voluntary "follow the money" initiatives for several years with various actors, including Google, to stop funding theft. Yet the same report found that Google's advertising technologies provided 51 percent of ads to pirate apps.[2] This is particularly alarming given that other digital advertisers "almost never appear on piracy apps."[3]

    a. Why was Google identified as the top major brand involved in placing advertising on applications? What measures are you taking to change this?

    b. Does Google receive money from placing advertising on websites that contain pirated content?

    c. What steps does Google take, both in the United States and worldwide, to prohibit advertising on piracy websites and applications?

    d. Do you agree that supporting commercial-scale pirate websites and apps through advertising dollars is wrong?

    e. Does Google, or its agents or subsidiaries, block payment for ad impressions on pirated content?

---

[1] Digital Citizens Alliance and White Bullet, *Breaking (B)ads: How Advertiser-Supported Piracy Helps Fuel A Booming Multi-Billion Dollar Illegal Market* (July 2021), https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf.
[2] *Id.*, pg. 34.
[3] *Id.*, pg. 17.

f. Does Google, or its agents or subsidiaries, conduct independent audits to ensure that any policies are being implemented effectively? How frequently are policies reviewed?

g. Does Google collect data over its own ad placements that would allow it to prevent placement on websites or apps that pose a high risk for distributing illegal content, including pirated content?

h. Google Ads is a tool offered to businesses and brands to place their ads in front of consumers. A brand chooses the type of audience it wants to reach and Google places the ad on the websites most likely to reach the target demographic. What steps are taken to ensure that ads are not placed on pirate websites?

i. What steps are taken to ensure that pirate publishers are prohibited from selling ad space through Google's advertising subsidiaries?

j. What steps is Google taking to enhance transparency of its activities on its advertising networks?

3. You stated in your testimony that Google does not sell data that it collects online.

   a. Does Google share data collected in one business unit with other business units?

   b. Does it share data collected with any legal entities outside of Google?

   c. Does it share any of this data in connection with a legal business transaction?

4. Ms. Slaiman advocates for "a digital regulator to comprehensively the policy questions surrounding digital platforms."
   a. Do you agree that this is necessary?
   b. Given the many issues beyond privacy and competition that address and implicate digital policy—including cybersecurity, national security, consumer rights, free speech, and intellectual property concerns—what existing agency would be the best situated, in your view, to carry out this role?
   c. Is it important to you that the regulator should be politically accountable?

Senator Blackburn
Questions for the Record to John Robb
The Global Guerrillas Report

1. It's imperative for the U.S. to get a national consumer privacy law in place—the EU and China have already done so. Given consumer concerns about how their data is being used online, what should that regime look like? What are obstacles the United States faces in getting to that point?

Senator Chuck E. Grassley

Questions for Mr. John Robb:

1. How important is the amount of data that a company has to their ability to effectively monetize that information?
2. How difficult can it be for a startup or small business to collect enough data to be able to compete with companies that have large amounts of data?
3. Some commentators argue that the amount of data currently possessed by large incumbent companies forecloses the ability of new entrants to compete. But, new data is being created every day and what data is important in the future may not be what is being collected today. If so, why isn't there an opportunity for additional companies to enter the market?
4. There is debate over whether Big Data should be regulated through the lens of consumer protection and privacy or whether antitrust laws should be used to address competition concerns with the collection of data. Do you have an opinion about the best approach to address this issue or should we be looking at a combination of different approaches?

Senator Tillis Questions for the Record – Big Data, Big Questions: Implications for Competition and Consumers

Mr. John Robb, Global Guerillas Report

1. The term "data" can have multiple meanings, which can sometimes generate confusion in policy discussions. How would you define "data" and "big data", as used in your written testimony?
    a. How would you define consumer and user data, specifically what would be included and excluded from these definitions?
    b. Would this include user uploaded videos, images, and text?
    c. Would such content be considered part of the "user" data, even if it includes content that originates from other sources?
    d. Does it include data in which intellectual property rights, including copyright, trade secret, trademark, or design rights, may subsist?
2. How would you differentiate your proposal for people to own data from existing intellectual property rights-based approaches?
3. You advocate for a new form of digital identity. Could you please explain further what you mean by this, and how you envision it working in the current environment? Are there particular technologies that would need to be developed for this to be implemented?
4. Ms. Slaiman advocates for "a digital regulator to comprehensively the policy questions surrounding digital platforms."
    a. Do you agree that this is necessary?
    b. Given the many issues beyond privacy and competition that address and implicate digital policy—including cybersecurity, national security, consumer rights, free speech, and intellectual property concerns—what existing agency would be the best situated, in your view, to carry out this role?
    c. Is it important to you that the regulator should be politically accountable?

Senator Blackburn
Questions for the Record to Steve Satterfield
Vice President of Privacy & Public Policy, Facebook

1. Please identify three distinct changes you have made to your platform to make it a safer and healthier experience for children.

Senator Chuck E. Grassley

Questions for Mr. Steve Satterfield:

1. Facebook monetize user's data by selling targeted advertisements. In the second quarter of 2021 Facebook had revenues of $29.08 billion. It has also been reported that the average American's data was worth $164 per year to Facebook. Is it accurate that the average America's data is worth $164 per year to Facebook?
2. There is debate over whether Big Data should be regulated through the lens of consumer protection and privacy or whether antitrust laws should be used to address competition concerns with the collection of data. Do you have an opinion about the best approach to address this issue or should we be looking at a combination of different approaches?

Senator Josh Hawley
Questions for the Record

Steve Satterfield
Vice President (Privacy and Public Policy), Facebook

1. **Please provide copies of all research findings or reports, whitepapers, slideshows, meeting recordings, or other documentation circulated within Facebook, over the past ten years, pertaining to each of the following topic areas:**

   a) **Addiction or addictive behaviors associated with the use of Facebook's products and services;**
   b) **Depression and/or self-harm associated with the use of Facebook's products and services;**
   c) **Impact of Facebook's products and services on the mental health and wellness of users under age 18;**
   d) **Extent to which Facebook's products and services are accessed by users under age 13**
   e) **Development of novel products or services targeted specifically to users under age 13.**

2. **Please provide the following information:**

   a) **How much revenue, in the aggregate, does Facebook estimate that it makes from users under 18?**
   b) **How much revenue does Facebook estimate that it makes from *each individual* user under 18?**
   c) **How much revenue, in the aggregate, does Facebook estimate that it makes from users under 13?**
   d) **How much revenue does Facebook estimate that it makes from *each individual* user under 13?**

3. **On September 27, Instagram head Adam Mosseri announced that the company was pausing efforts "to build an Instagram experience for people under the age**

of 13, often referred to as 'Instagram Kids,'" but "[stood] by the need to develop this experience" and intended "to work with parents, experts, policymakers and regulators, to listen to their concerns, and to demonstrate the value and importance of this project for younger teens online today."

a) When, if at all, does Facebook project that it will resume development on "an Instagram experience for people under the age of 13"?

b) On the basis of what considerations did Facebook conclude that it was more important to develop a designated digital space for users under 13 than, conversely, to ramp up efforts to prevent use of the platform by these users altogether?

Senator Tillis Questions for the Record – Big Data, Big Questions: Implications for Competition and Consumers

Steve Satterfield, Vice President, Privacy and Public Policy, Facebook

1. The term "data" can have multiple meanings, which can sometimes generate confusion in policy discussions. How would you define "data" and "big data", as used in your written testimony?
    a. How would you define consumer and user data, specifically what would be included and excluded from these definitions?
    b. Would this include user uploaded videos, images, and text?
    c. Would such content be considered part of the "user" data, even if it includes content that originates from other sources?
    d. Does it include data in which intellectual property rights, including copyright, trade secret, trademark, or design rights, may subsist?
2. Ad-revenue used to support online piracy is a longstanding problem. Criminals profit by receiving advertising dollars in exchange for giving users free access to stolen movies, music, books, software, and other materials—stealing money from hardworking creators, including many small businesses and individual artists. A recent report found that over *a billion dollars a year* in advertising goes to supporting online pirated content.[1] Both the US and EU have been working on voluntary "follow the money" initiatives for several years with various actors, including Facebook, to stop funding theft. Yet the same report found that Facebook was a top ad spender, accounting for 27% of major brand advertising appearing on piracy apps.[2] This is particularly alarming given that other digital advertisers "almost never appear on piracy apps."[3]
    a. What steps does Facebook take, both in the United States and worldwide, to prohibit advertising on piracy websites and applications?
    b. Why was Facebook identified as the top major brands involved in placing advertising on applications? What measures is Facebook taking to change this?
    c. Does Facebook agree that supporting commercial-scale pirate websites and apps through advertising dollars is wrong?
    d. Does Facebook, or its agents or subsidiaries, identify websites or apps that pose a risk of distributing or displaying copyright protected content without authorization?
    e. Does Facebook, or its agents or subsidiaries, restrict the display of its advertisements on websites that infringe copyright, or pose a high risk of engaging in copyright infringement?
    f. Does Facebook, or its agents or subsidiaries, block payment for ad impressions on pirated content?

---

[1] Digital Citizens Alliance and White Bullet, *Breaking (B)ads: How Advertiser-Supported Piracy Helps Fuel A Booming Multi-Billion Dollar Illegal Market* (July 2021), https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf.
[2] *Id.*, pg. 17.
[3] *Id.*, pg. 17.

g. Does Facebook, or its agents or subsidiaries, conduct independent audits to ensure that any policies are being implemented effectively? How frequently are policies reviewed?
h. Does Facebook collect data over its own ad placements that would allow it to prevent placement on websites or apps that pose a high risk for distributing illegal content, including pirated content?
i. What steps is Facebook taking to enhance transparency of its activities on its advertising networks?

3. Your written testimony states that there are "always risks when people transfer data online." Please elaborate on the nature and scope of these risks, and the people and entities who are implicated by these risks.

    a. What steps does Facebook take to inform others of these risks?
    b. How does the Data Transfer Project address these risks?

4. Ms. Slaiman advocates for "a digital regulator to comprehensively the policy questions surrounding digital platforms."
    a. Do you agree that this is necessary?
    b. Given the many issues beyond privacy and competition that address and implicate digital policy—including cybersecurity, national security, consumer rights, free speech, and intellectual property concerns—what existing agency would be the best situated, in your view, to carry out this role?
    c. Is it important to you that the regulator should be politically accountable?

Senator Chuck E. Grassley

Questions for Ms. Charlotte Slaiman:

1. How important is the amount of data that a company has to their ability to effectively monetize that information?
2. How difficult can it be for a startup or small business to collect enough data to be able to compete with companies that have large amounts of data?
3. Some commentators argue that the amount of data currently possessed by large incumbent companies forecloses the ability of new entrants to compete. But, new data is being created every day and what data is important in the future may not be what is being collected today. If so, why isn't there an opportunity for additional companies to enter the market?
4. There is debate over whether Big Data should be regulated through the lens of consumer protection and privacy or whether antitrust laws should be used to address competition concerns with the collection of data. Do you have an opinion about the best approach to address this issue or should we be looking at a combination of different approaches?

Senator Tillis Questions for the Record – Big Data, Big Questions: Implications for Competition and Consumers

Charlotte Slaiman, Competition Policy Director, Public Knowledge

1. The term "data" can have multiple meanings, which can sometimes generate confusion in policy discussions. How would you define "data" and "big data", as used in your written testimony?
    a. How would you define consumer and user data, specifically what would be included and excluded from these definitions? For example, the section of data portability refers to "your data" – what would this include?
    b. Would this include user uploaded videos, images, and text?
    c. Would such content be considered part of the "user" data, even if it includes content that originates from other sources?
    d. Does it include data in which intellectual property rights, including copyright, trade secret, trademark, or design rights, may subsist?
2. Your testimony advocates for "a digital regulator to comprehensively the policy questions surrounding digital platforms."
    a. Given the many issues beyond privacy and competition that address and implicate digital policy—including cybersecurity, national security, consumer rights, free speech, and intellectual property concerns—what existing agency would be the best situated, in your view, to carry out this role?
    b. Is it important to you that the regulator should be politically accountable?
3. Your testimony refers to data portability as an important tool "to neutralize the power that Big Data confers upon dominant digital platforms."
    a. In your view, is the Data Transfer Project, described in Google's testimony as a partnership among Google, Apple, Facebook, Microsoft, and Smugmug, an acceptable way to address data portability?

Senator Grassley
Questions for the Record – Big Data, Big Questions: Implications for Competition and Consumers
Sheila Colclasure, Global Chief Digital Responsibility and Public Policy Officer, IPG Kinesso

1. **There is debate over whether Big Data should be regulated through the lens of consumer protection and privacy or whether antitrust laws should be used to address competition concerns with the collection of data. Do you have an opinion about the best approach to address this issue or should we be looking at a combination of different approaches?**

Response to Senator Grassley:

In our modern American economy, any data privacy law is also competition law. Both privacy and competition concerns have data availability, use, and control at their core. For businesses of all sizes, but especially small business and new entrants, access to data is the dependent factor on whether the business can compete or not. Companies may have better technology, better ideas, and innovation at their core, yet without access to data, they cannot compete.

Recently introduced data privacy legislation, as drafted, would have a catastrophic impact on competition because it restricts who can collect, control, and use data. This effectively picks winners and losers, consolidating market power into the hands of a few massive, Big Tech, data holders. In many ways, Big Tech is like a basic consumer utility, like water and energy. Big Tech has grown data-dominant relatively unimpeded, offering functionality to people that has become ubiquitous with our daily lives, giving these companies tremendous market power to gain consumer consent for the collection of their data.

There has been much debate about consumer consent versus other data regulatory approaches such as fair, open, and accountable data flow and use. While consumer consent is important, and a laudable goal, it alone is an insufficient model in the complex digital ecosystem of data infinity and tech certainty. Data is essential to all market players, especially small business, new business, and our innovators. By writing laws that grant control of data to a few companies that get to the consumer first, we create economic winners and losers. Such laws would effectively grant data access to some and deny it for others. This approach frustrates free and fair competition among all of the players in the ecosystem.

We are beyond the point where it is possible to pass a data privacy law that does not also – whether explicitly or by omission – affect competition. The reality is that today's connected marketplace is dominated by companies who were able to thrive and grow, thanks in part to ready access to consumer data. A comprehensive federal privacy law that in practical effect limits consumer data to just a few dominant players risks concentrating even more power in the hands of a few, giving more exclusive control of

data about people to a few. In our data-intense economy, this precludes robust competition, vibrant innovation, and the possibility of the small company becoming connected, finding its audience, and serving its audience competitively. We emphasize the essential nature of data availability, open data flow, and fair uses of data to innovation, competition, and a vibrant ecosystem of connected market participants. We contend that a federal data privacy law and a competition law should be complementary and provide for responsible and accountable data sharing so that everyone can compete on a level playing field.

We urge the Committee to consider the effect that mergers have had on control of the consumer data value chain, and thus on competition. Traditional antitrust analysis has focused on the effect of mergers in a specific consumer-facing market, but the enhancement of dominant data positions plays a large role in the acquisition strategy of the dominant online platforms. We hope this Committee will recognize the essential nature of data to our entire connected economy and the ecosystem of companies that enable our connected marketplace.

In order to protect people, promote the fair use of their data, and support a robust, trustworthy and competitive connected marketplace, a federal privacy law should be drafted in a way that protects and enables competition. It should promote fundamental privacy rights for consumers and enable responsible and accountable use and sharing of consumer data by commercial enterprises. This allows the market to continue to provide a wide array of benefits to people including things like safer online payments, ready access to business and consumer credit, access to free content and platforms, and cost efficient and effective advertising for all, especially small businesses, and new market entrants.

We at IPG have built accountability and responsible data practices into everything we do. We believe that corporate America is ready to responsibly collect and share consumer data and be accountable for its actions in doing so. We encourage the Committee to protect the fair and open use of data as fundamental to competition. We urge the Committee to help develop a federal privacy law that is future-fit for the realities of the Digital Age, protects consumers, and enables a connected marketplace in which all participants can compete fairly, so long as they engage in safe and accountable data use and sharing.

Senator Ossoff
Questions for the Record – Big Data, Big Questions: Implications for Competition and Consumers
Sheila Colclasure, Global Chief Digital Responsibility and Public Policy Officer, IPG Kinesso

1. **Please list any instance where any IPG company provides or has ever provided products or services to any federal agency, or to any federal prime contractor or federal subcontractor for purposes of supporting a federal program, including the nature and value of the products or services provided. As part of this response, please describe the nature of Acxiom's 2019 contract with the United States Special Operations Command, including how Acxiom supports "Project Red Mouse." If necessary, submit a classified annex to the Committee on the Judiciary to ensure this information responsive to this question is complete.**

At the outset, it is important to note that the Interpublic Group of Companies, Inc. (IPG) is a holding company compromised of roughly 90 different companies, the vast majority of which are creative advertising agencies. For purposes of these responses, I have limited my response to the two principal data and technology companies within IPG: Acxiom and Kinesso. Moreover, given the limited availability of some historical records, the resources that would be required to undertake a comprehensive search, and my desire to respond with confidence based on records that we do have, I have limited our investigation and responses to facts going back to 2017. Kinesso was launched in 2019 and so my responses specifically applicable to Kinesso go back to that date. With that understanding, I offer the following responses to the QFRs.

Response to QFR 1: Kinesso has not provided products or services to any federal agency or to any federal prime contractor or federal subcontractor for purposes of supporting a federal program. Acxiom has performed occasional work with federal agencies, such as analytic programs with the Department of Veterans Affairs, Office of Enterprise Integration (OEI). OEI's primary goal is to utilize data and analytics to develop insights that enable VA programs to better connect with veterans and strengthen the VA's delivery of services and benefits to veterans, their families, survivors, and caregivers. The accuracy and reliability of that data is critical to the success of the mission. Acxiom serves as a subcontractor to the prime contractor and provides Data Products and Information Services as part of that relationship. (Data Products and Information Services are defined in response to QFR 7 below.)
Acxiom provides consulting services to the United States Department of State Visa and Passport Analysis Branch (VPAB) in Diplomatic Security, pursuant to GSA Schedule 70. Our relationship began with a strategic consulting assessment focused upon information assets and resources related to VPAB's Investigative Management System (IMS). IMS is the central repository and user portal for all State Department investigative cases, predominantly visa and passport fraud. Acxiom's primary goal is to assist the State Department in making IMS a more accurate and complete investigation solution for its

agents and analysts. Acxiom provides consulting services only and does not provide any Data Products or Information Services as part of that relationship.

Finally, Acxiom is not at liberty to confirm or deny the existence of any classified agreement or to discuss any other work the company may do on a classified basis for agencies of the United States Government. We recommend the Committee contact U.S. Special Operations Command or other appropriate resources within the United States Government if additional information is needed on any classified initiative.

2. **Please list any instance where any IPG company provides or has ever provided products or services to any state or local law enforcement agency**.

Response to QFR 2: Based on our investigation, neither Kinesso nor Acxiom has bid for, or provided any products or services to state or local law enforcement agencies since 2017.

3. **Please list all bids for federal contracts submitted by any IPG company, even if such bids were unsuccessful. Specify the federal agency, the title and purpose of the bid, the products or services that were to be provided, and where applicable the estimated or suggested value of the contract(s).**

Response to QFR 3: As there does not appear to be a public database or reliable comprehensive resource that tracks bidding on federal contracts, research for this question proved difficult. In addition to the work we perform for the Veterans Administration mentioned in Response to QFR 1 as a sub-contractor to Sierra7 (prior to that, the prime contractor was HMS Technologies, Inc.), we identified four additional bids to federal agencies:

Year	Agency	Purpose	Products/Services	Value	Bid Status
2018	DMDC	Identity Verification	Data and Data Processing	$275,000	Lost
2018	Login.gov	Identity Verification	Data and Data Processing	$25,000	Lost
2020	HHS	Digital Activation of Vaccine Campaign	Data and Data Processing	$625,000	Lost
2020	Defense Health Agency	Information Management	Consulting	$1.1 million	Lost

4. **Please list all bids for contracts with state or local law enforcement agencies submitted by any IPG company, even if such bids were**

unsuccessful. Specify the agency, the title and purpose of the bid, the products or services that were to be provided, and where applicable the estimated or suggested value of the contract(s).

Response to QFR 4: As indicated in response to QFR 2, we did not find any instances where Acxiom or Kinesso bid on state or local law enforcement work since 2017.

5. **Please describe any instance where any IPG company provides any product or service to any foreign governmental entity, foreign state-owned enterprise, or foreign political entity (e.g., foreign political parties, political candidates, or political campaigns).**

Response to QFR 5: Kinesso in the US has not provided a product or service to any foreign government entity, foreign state-owned enterprise, or foreign political entity since 2019. Acxiom has performed small data enhancement projects (i.e., two projects for under $100,000 total), for a Caribbean tourism authority. A sister company, Acxiom Ltd. (UK), has provided information services to the UK Information Commissioner's Office (UK Data Protection Authority). We cannot rule out situations where Acxiom or Kinesso may have provided products or services to an entity that is wholly or partially owned by a foreign government (e.g., a national airline), however, no such entity was readily apparent while we performed our research.

6. **Please describe any instance where any IPG company provides or has provided any product or service to any foreign or U.S. business for purposes of supporting that business' contract work on behalf of any foreign governmental entity**.

Response to QFR 6: It is important to note that data ethics is integral to everything we do. For more than two decades, we have focused on the sources of our data, how it is used, and whether both of those complied with law and were consistent with our ethical data framework. We have extensive systems and policies and procedures in place to make sure that this is the case. While it is possible that one of our clients used our products and services for purposes for purposes of supporting its work on behalf of a foreign governmental entity, our investigation failed to identify any instance where we knew about this type of service when it was contracted for, and we have not identified any instance since 2017 where this occurred.

7. **Please describe any relationship through which any IPG company receives personally identifiable data or any data pertaining to U.S. persons from federal, state, or local governments or government agencies. As part of this response, please describe whether data received includes information about the online presence of individuals, such as social media accounts.**

Response to QFR 7: Kinesso does not directly license personally identifiable data or data pertaining to US persons from federal, state, or local governments or government agencies. Acxiom serves as the primary data sourcing entity for Kinesso.

Acxiom has two primary lines of business. The first line of business is referred to as "information services," which includes sophisticated database administration services to improve the useability of data that Acxiom's clients provide. The second line of Acxiom's business is data products, where Acxiom provides data to its clients for their (and in the case of an Acxiom data reseller, their end users'), internal use. Acxiom licenses public records such as voter records, hunting/fishing licenses, and real estate transactions, for its data products. All of this information is publicly available, and if its use is restricted in any way by a statute or by the licensor, we conform our use and distribution of that data with those restrictions and our own guidelines.

8. **Please describe in detail the sources from which Acxiom or other IPG companies obtain unique device identifiers, including IMEI, IMSI, MAC addresses, or IDFA/Ad-IDs.**

    a. **If you receive or obtain unique identifiers from commercial partners, please describe the means by which those partners obtained the identifiers.**

Response to QFR 8: Acxiom and Kinesso collect Mobile Ad IDs (MAIDs) via a licensed file from SDK providers. We do not receive lat/long or IP addresses in combination with those MAIDs. We do not incorporate the MAIDs into any other product, but we do provide them to third parties as a data product. Consistent with our overall ethical data framework, we require that the source of this information represent and warrant their compliance with laws and applicable industry practices when they provide us the data and we have a program in place to confirm that their sources have not changed and these fundamental representations remain in place on an annual basis.

9. **Please describe efforts by any IPG company to link unique device identifiers with the IP addresses of residential or commercial internet connections.**

Response to QFR 9: Acxiom and Kinesso have not traditionally offered this type of product, nor do we currently have any commercial offerings where we link device identifiers to IP addresses. Given client interest and demand, we are exploring this potential opportunity from a commercial and regulatory perspective. If we decide to move forward and offer a commercial product that links unique device identifiers with IP commercial or residential addresses, it will be legal under all applicable laws and will also comply with our ethical data framework, which verifies the source and the intended use of the data on a client- by-client basis.

10. **Please describe any products or services any IPG company offers to clients to enable them to see connections between personally identifiable data, such as SSN, home address, email address, or telephone number, and sensitive data, such as web browsing activity, web search history, or purchase history.**

Response to QFR 10: Acxiom offers its "Real Identity" product, which performs a valuable function for Acxiom's clients. Real Identity allows Acxiom's clients to synchronize identity data (e.g., name, home and email address, and telephone number) used across the client's enterprise. By synthesizing and analyzing billions of customer transactions and interactions, both digitally and offline, Real Identity allows Acxiom's clients to build and maintain first-party identity graphs to recognize individuals and build deeper customer relationships across their full enterprise.

Importantly, this service is only used to build first party data graphs for our clients, the data flowing through this service is not added to any Acxiom third-party data graph. So, whether it is the client using the product on its own behalf or Acxiom providing those services as the client's processor, the client's own data or ethically sourced, third-party data licensed by our client is used to make these connections in accordance with the client's own privacy policy and the client's notice to consumers of the potential for re-identification.

Lastly, it is also important to state that Acxiom and Kinesso do not offer products or services to clients that enable them to see connections between personally identifiable data and sensitive data, such as SSN, web browsing activity, or web search history, that is not already in their possession. Acxiom does license consumer purchase behavior data that is associated to personally identifiable information. However, that data is categorical (e.g., clothing, hardware); not at an item/SKU level of granularity, nor is it associated to the specific location that the purchase was made.

11. Please describe any contractual limitations Acxiom places on entities' use or disclosure of data about individuals.

   a. Does Acxiom monitor its clients for contract adherence? If so, how?
   b. Has Acxiom or any other IPG company discovered or become aware of a contracting partner's contractual breach relating to personally identifiable information? If so, please describe any resulting actions taken by IPG or an IPG company.

Response to QFR 11: Acxiom's client contracts require clients to comply with all applicable laws and restrict the use of data and services for client to internal business purposes. Acxiom includes similar flow-down obligations through restrictions in its contracts with resellers and data brokers (so that their customers are subject to the same restrictions). This is central to how we conduct our business and how we have conducted it over the last three decades. It is part of our internal ethical data framework.

In addition to contractual restrictions, Acxiom has a due diligence team that confirms who our client are and what they do (to the extent, their business can be determined). That team also reviews compliance with our client contracts, including data use provisions in the contracts. It is impossible to confirm compliance with every client contract, so reviews are done on a systematic basis to sample compliance across our

user base. We also follow up on any credible information we receive regarding potential non-compliance with our agreements.

Acxiom has business interactions with many clients that can be described as "high touch" and "long-term" information services. In these situations, Acxiom has a close working relationship with the particular client over a long period of time. These types of relationships afford greater visibility into the manner in which the client uses our products and services, allowing greater confidence regarding their compliance with contractual restrictions in those situations.

12. Other than its website, what steps does Acxiom take to alert consumers to their ability to opt out of the company's use of their data?

a. Do you treat opt-out requests from California residents differently than opt-out requests from residents of other state?
b. If so, please describe any differences in how Acxiom would treat data about a person from California after receiving an opt-out request, compared to how it would treat data about a person from another state who submitted an opt-out request.

Response to QFR 12: Acxiom provides CCPA rights to all individuals in the United States. Acxiom does not treat California residents differently from an opt out (or any other data rights perspective), than any other resident of the United States.

Acxiom works hard to provide as much educational information to consumers as possible. We have extensive information available on our website, but in addition, we promote consumer awareness in media interactions and in consumer oriented educational activities (e.g., conferences, seminars, and consumer group sponsorships).

Senator Tillis
Questions for the Record – Big Data, Big Questions: Implications for Competition and Consumers
Sheila Colclasure, Global Chief Digital Responsibility and Public Policy Officer, IPG Kinesso

1. **The term "data" can have multiple meanings, which can sometimes generate confusion in policy discussions. How would you define "data" and "big data", as used in your written testimony?**
    a. **How would you define consumer and user data, specifically what would be included and excluded from these definitions?**
    b. **Would this include user uploaded videos, images, and text?**
    c. **Would such content be considered part of the "user" data, even if it includes content that originates from other sources?**
    d. **Does it include data in which intellectual property rights, including copyright, trade secret, trademark, or design rights, may subsist?**

Response to Senator Tillis:

The fact that humans use data in so many different ways is part of what makes legislating with respect to data issues so difficult. Policymakers generally want to preserve and foster beneficial data uses while limiting harmful ones. The unique purpose for which data is being regulated should help define the term – and different inclusions or exclusions may be needed within the scope of a single bill.

You specifically asked how I would define the term "data" "as used in my written testimony." I was asked to testify about how my company competes in data-driven marketing as compared to others, specifically first-party platforms. The main data that matters for the purposes of that competition is not user-generated content, such as you describe above. Such data may be of interest to others, but not to us. However, user-generated digital history – product search information, for example – is useful for marketing, and therefore access to it is relevant to competition issues. Again, Congress should consider the purpose it intends to effectuate in determining the scope of defined terms.

Data may be protected by intellectual property rights in and of itself, or it may be processed by use of algorithms or processes that themselves constitute IP, in which case the resulting product may contain protectable IP. However, IP protections are not incompatible with any of privacy, competition and the enforcement of antitrust laws.

2. **Your testimony advocates for an expansive view of competition law that would account for the flexibility to account for data-related issues, and advocates for the Committee to consider privacy and competition to be interrelated.**

a. **Would the same consideration be extended to other "big data" issues, such as intellectual property rights, cybersecurity, national security, data protection, and other issues?**

b. **How should antitrust law be tailored to appropriately account for privacy rights, or other legitimate concerns such as intellectual property rights?**

Response to Senator Tillis:

I did advocate for the Committee to consider privacy and competition to be interrelated, and in the context of the hearing, which related to S. 2992, I stand by that recommendation. I did not, and did not intend, to advocate for an expansive view of antitrust law, and therefore underscore my suggestion that the Committee "consider privacy and competition not as separate bodies of law, but instead to be interrelated." A better statement would be that in the context of this legislation, antitrust and privacy become interrelated. If Congress is going to regulate competition, it should consider the privacy implications of doing so, and vice versa. Congress should consider the other interests you mention, as well.

The ability to access data that consumers are making available about themselves is key to competition in today's markets. Legislation that would regulate competition in digital markets must recognize this, and so must legislation that would protect privacy by regulating use of consumer data.

3. **Ms. Slaiman advocates for "a digital regulator to comprehensively [regulate] the policy questions surrounding digital platforms."**

   a. **Do you agree that this is necessary?**

   b. **Given the many issues beyond privacy and competition that address and implicate digital policy—including cybersecurity, national security, consumer rights, free speech, and intellectual property concerns—what existing agency would be the best situated, in your view, to carry out this role?**

   c. **Is it important to you that the regulator should be politically accountable?**

Response to Senator Tillis:

We support enactment of a national privacy law, with enforcement by the FTC and state attorneys general. We also support resourcing the FTC appropriately to conduct this expanded mission. We do not have a position on whether it is necessary to have a regulator specific to digital platforms.

For privacy regulation, the best situated agency is the FTC, because it has developed experience and expertise. We do not oppose creation of a Bureau of Privacy in the FTC. Privacy regulation primarily impacts the commercial sector, and as a commercial regulator, the FTC is well-positioned.

I would also add that, as demonstrated by the August 11, 2022, FTC Advanced Notice of Proposed Rulemaking, federal legislation is necessary to prevent FTC overreach and to ensure that the FTC develop rules pursuant to congressional authorization and consistent with congressional intent.

Senator Blackburn
Questions for the Record – Big Data, Big Questions: Implications for Competition and Consumers
Sheila Colclasure, Global Chief Digital Responsibility and Public Policy Officer, IPG Kinesso

It's imperative for the U.S. to get a national consumer privacy law in place – the EU and China have already done so. Given consumer concerns about how their data is being used online, what should that regime look like? What are the obstacles the United States faces in getting to that point?

Response to Senator Blackburn:

While many proponents of a national privacy law point to the EU General Data Protection Regulation as a model for the United States, Congress can, and should, do better. Studies since the GDPR went into effect in 2018 make clear that the GDPR has had a severe negative effect on the European economic market, including suppressing competition and consolidating market power into the large gate-keeper technology platforms. See, e.g., "GDPR Cost Businesses 8% of Their Profits, According to A New Estimate," https://techmonitor.ai/policy/privacy-and-data-protection/gdpr-cost-businesses-8-of-their-profits-according-to-a-new-estimate. It is also clear that the GDPR has not been able to adjust to the rapid change of innovation. In part for these reasons, both the European Union and the UK are already considering a major overhaul of their GDPR legislation. "UK Pauses Data Reform Bill to Rethink How to Replace GDPR," https://techcrunch.com/2022/10/03/uk-data-reform-bill-replace-gdpr/. In fact, GDPR has had such anticompetitive effects that the EU has introduced five additional pieces of legislation to attempt to better govern the big gatekeepers and the realities of data and algorithms in the Digital Age. "A Europe Fit for the Digital Age," https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en. The EU's difficulties with GDPR demonstrate that it should not serve as model for the U.S. Contrary to GDPR, U.S. privacy legislation should protect data-driven business practices, while providing meaningful redress to Americans who suffer actual harm through violation of their privacy rights.

The U.S. should restore its leadership role on the global stage with a forward-thinking, future-fit approach. Congress should consider a bill that focuses on harm prevention and accountability. The law should prohibit certain uses of data that are per se unfair, such as fraud, unlawful discrimination, stalking, and harassment, and expressly permit the collection, sharing, and use of data for beneficial uses including advertising and marketing purposes. The policy principles championed by the Privacy for America coalition are incredibly instructive and should be fully adopted in any national privacy law. https://www.privacyforamerica.com. Additionally, the Information Accountability Foundation has developed model legislation, The FAIR and OPEN USE Act, that would be better for America and better for Americans.
https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-

content/uploads/2021/05/FAIR-and-OPEN-USE-Act-May-26-2021-1.pdf?time=1622546970.

The U.S. should also consider the model of Singapore, which has enacted a national privacy law that leads to accountability without unnecessarily hampering the flow of information or favoring certain market participants in the information economy over others. https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act. The law, which was drafted in consultation with The Information Accountability Foundation and the Center for Information Policy Leadership addresses the practicalities of the digital future, and ensures robust, competitive and trustworthy economy. Essentially, the law says, "let data flow for beneficial uses, but be accountable to detect and prevent harms."

In addition to adopting a harms-based approach, a federal privacy law must resolve two issues that are relatively unique to the U.S. system: state law preemption and the scope of any private right of action.

If federal privacy legislation is to ensure future a competitive digital economy, it must include a provision that broadly preempts recent and future state forays into the use of personal information for marketing and advertising. Given the importance of advertising to the U.S economy and the fact that advertising also directly subsidizes valuable services and free speech activities on the Internet, a comprehensive national privacy law should expressly indicate Congress' intent to occupy the field. Without a strong preemption provision, the national law simply becomes yet another law that companies must navigate, creating uncertainty, operational inconsistencies, and administrative costs that are passed right back to consumers in the form of increased costs of goods and services and less access to knowledge, news, and the connected marketplace. The inevitable differences in these state level laws creates administrative and financial burdens that divert important resources that can be otherwise devoted to innovation and will substantially restrict companies' ability to grow.

More specifically, a well-drafted preemption provision would expressly preempt states and state subdivisions from adopting, maintaining, or enforcing a state law or regulation that relates to the subject matter of the national privacy law or any regulation promulgated by the national privacy law. Similarly, to remove any potential ambiguity, the national privacy law should explicitly reference and preempt the California Consumer Privacy Act, as amended by the California Privacy Rights Act, Cal. Civ. Code §1798.100 et seq., the Virginia Consumer Data Protection Act, Va. Code Ann. §59.1-580 et seq., the Colorado Privacy Act, Co. Rev. Stat. 6-1-1301 et seq., the Utah Privacy Act, Utah Code Ann. §13-61-101 et seq., and the Connecticut act concerning personal data privacy and online monitoring, 2022 Ct. SB 6, as well as any regulations implementing those statutes.

The second major obstacle to a national privacy law is whether to include a private right of action, especially if that right includes statutory damages. As we saw with other state and federal statutes that include a private right of action with a statutory damage

component, (e.g., the Fair Credit Reporting Act, the Telephone Consumer Protection Act, and the Michigan Video Rental Privacy Act), lawyers brought a number of class action cases seeking astronomical statutory damages even though the consumers objectively did not suffer actual harm. See, e.g., TransUnion v. Ramirez, 141 S.Ct. 2190 (2021).

Many companies are willing to accept a limited ability to sue to recover actual damages, provided the resulting privacy law includes a corresponding strong preemption provision. Without a correspondingly strong preemption provision, companies have continued exposure to causes of action under state law that likely include significant administrative penalties under those laws (e.g., the California Privacy Rights Act), as well as class action lawsuits for statutory damages under state laws. Such a situation is untenable and would undo any efforts by Congress to institute and enable digital innovation, while protecting privacy and competition.

Responses to Questions for the Record
U.S. Senate Committee on the Judiciary
Subcommittee on Competition Policy, Antitrust, and Consumer Rights
"Big Data, Big Questions: Implications for Competition and Consumers"
September 21, 2021

Markham Erickson
Vice President Of Government Affairs And Public Policy, Google, Inc.

Written Questions Submitted by Sen. Grassley to Markham Erickson:

Question 1. Google monetizes user's data by selling targeted advertisements. In the second quarter of 2021 Google had advertising revenues of $50.44 billion. How much is the average American's data worth to Google?

Google does not sell users' personal information. That is not our business model, and we have always made this policy a touchstone of Google's relationship with our users.

Google provides users with a range of controls over how their information is used, including for personalized ads. Users may opt to permit Google to personalize the ads they see using their activity and account data, but services like Search, Maps, Gmail, and Drive remain free for users who choose not to allow the use of their data for ad targeting. Indeed, ads on Google Search primarily rely on the context of the current search query to select ads, not user information. A user can see how ads are personalized to them and change their advertising settings at https://adssettings.google.com/. Users can also learn about Google's collection and use of data through our industry-leading, in-context notices, privacy reminders, and of course our Privacy Policy (available at https://policies.google.com/privacy).

Information regarding revenue generated by Google, by segment and source, is disclosed on a quarterly and annual basis in our Forms 10-K and 10-Q. Recent filings are available at https://abc.xyz/investor/.

Question 2. There is debate over whether Big Data should be regulated through the lens of consumer protection and privacy or whether antitrust laws should be used to address competition concerns with the collection of data. Do you have an opinion about the best approach to address this issue or should we be looking at a combination of different approaches?

We recognize policymakers and regulators are working to protect privacy while also considering whether making more data available among competitors would increase competition. These are complex issues, but we are encouraged to see some privacy and

competition regulators working together to contribute their relevant expertise to the important questions being considered, including when a privacy-oriented practice is being evaluated in an antitrust context. We will continue to engage with policymakers and regulators, as well as other stakeholders, to support thoughtful regulation that encourages innovation and protects consumers. For example, we continue to publicly support federal privacy legislation in the United States (for more information, please see https://blog.google/outreach-initiatives/public-policy/the-urgent-necessity-of-enacting-a-national-privacy-law/).

Written Questions Submitted by Sen. Hawley to Markham Erickson:

Question 1. Please provide copies of all research findings or reports, whitepapers, slideshows, meeting recordings, or other documentation circulated within Google, over the past ten years, pertaining to each of the following topic areas:

a. **Addiction or addictive behaviors associated with the use of Google's products and services;**

b. **Depression and/or self-harm associated with the use of Google's products and services;**

c. **Impact of Google's products and services on the mental health and wellness of users under age 18;**

d. **Extent to which Google's products and services are accessed by users under age 13;**

e. **Development of novel products or services targeted specifically to users under age 13.**

The relationship between technology use and physical and mental wellbeing is complex, especially for children and young people. Recent studies have highlighted that digital media use can help teens communicate with peers and family, seek helpful resources and support if they are experiencing distress, and find opportunities for learning and entertainment that can help combat isolation. We partner with expert organizations to inform our products and policies, and directly support and provide expertise to organizations that work directly with young people. Through Google.org, we have supported several organizations that support child and teen mental health, providing funding and technical expertise.

We take the health and well-being of all our creators and viewers seriously. Awareness and understanding of mental health is important and we support creators sharing their stories, such as posting content discussing their experiences with depression, self-harm, or other mental health issues. For much of this content, we show viewers viewers where they can find mental health support or suicide prevention resources, like referring them to the 24/7 Crisis Lifeline here in the US. However, we do not allow content that promotes self-harm or suicide.

Over the past several years, as part of our work to build a trusted environment for kids and families, we have worked with parents and experts across the globe in areas related to child safety, child development, digital literacy, and online safety. The advice from this group of trusted experts helps us build products that offer a positive experience for families, and was instrumental in the creation of the YouTube supervised experience, a solution for parents of teens and tweens launched in March 2021 on the main YouTube platform.

The YouTube supervised experience allows parents to choose among three different content choices: content generally suitable for viewers aged 9+; content generally suitable for viewers 13+; and the 'Most of YouTube' option, which excludes all age-restricted content (18+). To help parents understand more about the YouTube supervised experience, we have developed guides (such as those available at https://www.youtube.com/myfamily/), videos (such as https://www.youtube.com/watch?v=oVOa6nDU7HQ), and support pages (available at https://support.google.com/youtube/answer/10314940?hl=en), building on Google's successful Be Internet Awesome digital literacy resources, and in partnership with the National PTA, Parent Zone UK and other leading experts. We will continue to partner with these and other groups to provide easy to use resources specifically for parents to help them keep their kids safe online.

For our youngest users, we've also built a dedicated kids destination, the YouTube Kids app. We've invested heavily over the years to make YouTube Kids a safer, family-friendly place for kids to explore their imagination and curiosity. We have a higher bar for which videos can be a part of the app and also empower parents to control what content their child can and cannot see. If a channel has "Made for Kids" content, we use YouTube's quality principles for kids and family content to determine the monetization status of that content. We also have a made for kids ads policies to ensure we are providing protections and delivering age-appropriate experiences for ads on Google and we do not allow personalized targeting to kids under 13.

We care deeply about how families and children use technology and have engaged third parties to help us understand the challenges faced. For example, in 2019, we commissioned Fluent Research to conduct a study to examine the role digital technology plays in the wellbeing of families and to help us understand how we could better support healthy tech habits through our products (more information is available at https://services.google.com/fh/files/blogs/fluent_digital_wellbeing_report_global.pdf). This research, which included focus groups and/or survey respondents in eleven countries, has informed our approach to product and policy design, directly impacting our efforts to create experiences that help develop healthy tech habits, including the evolution of Family Link parental controls.

Question 2. Please provide the following information:

a. **How much revenue, in the aggregate, does Google estimate that it makes from users under 18?**

b. **How much revenue does Google estimate that it makes from *each individual* user under 18?**

c. **How much revenue, in the aggregate, does Google estimate that it makes from users under 13?**

d. How much revenue does Google estimate that it makes from *each individual* user under 13?

Google does not maintain, in the ordinary course of business, records of revenues at the user level. Our quarterly and yearly operating income numbers for all our business units are detailed in our public filings, available at https://abc.xyz/investor/.

Question 3. Has Google ever required a third party to alter search results, provide internal data, or make other nonmonetary contractual concessions in order to distribute or otherwise obtain access to Google's apps, including YouTube and YouTube TV?

Our agreements to distribute YouTube include a certification process in which new devices need to meet our technical requirements. This process exists to provide a consistent and high-quality YouTube experience for users across different devices.

For distribution partners whose devices provide users with a universal search experience that aggregates results across multiple content providers, YouTube requires that search results from YouTube are included among the results from other content providers. Partners have complete control on where to display the YouTube search results. Other content providers have similar requirements.

What is different about YouTube — in contrast to other content providers — is that we have an incredibly expansive content library with 500 hours uploaded every minute. YouTube makes a public Application Programming Interface (API) available so that all partners can query that API when a user issues a search query. If distribution partners do not have a universal search feature, we do not require them to display YouTube search results.

Written Questions Submitted by Sen. Tillis to Markham Erickson:

Question 1. The term "data" can have multiple meanings, which can sometimes generate confusion in policy discussions. For example you refer to the publicly available web as an important data set. How would you define "data" and "big data", as used in your written testimony?

a. **How would you define consumer and user data, specifically what would be included and excluded from these definitions? For example, the section of data portability refers to the ability of users to export "their data".**

b. **Would this include user uploaded videos, images, and text?**

c. **Would such content be considered part of the "user" data, even if it includes content that originates from other sources?**

d. **Does it include data in which intellectual property rights, including copyright, trade secret, trademark, or design rights, may subsist?**

Google's Privacy Policy (available at https://policies.google.com/privacy) explains what information Google collects, why Google collects it, and how users can update, manage, export, and delete their information. We are committed to giving users access and control over their data. We were one of the first companies to offer users a centralized portal to see and manage their data through easy-to-use tools with the launch of MyAccount in 2015 (now Google Account), and we encourage Google users to visit their Google Account (available at https://myaccount.google.com/) where they can review the data Google has collected and can choose to export or delete the data we store.

Our Privacy Policy describes in detail the categories of information we collect. The most common of these include:

- Identifiers such as name, phone number, and address, as well as unique identifiers tied to the browser, application, or device used.
- Demographic information, such as age, gender, and language.
- Commercial information such as payment information and a history of purchases made on Google's services.
- Internet, network, and other activity information such as search terms; views and interactions with content and ads; and activity on third-party sites and apps that use our services.
- Geolocation data, such as may be determined by GPS, IP address, and other data from sensors on or around a user's device, depending in part on the device and account settings.
- Other information created or provided by users, such as the content created, uploaded, or received (like photos, videos, emails, docs, or spreadsheets).

- Inferences drawn from the above, like ads interest categories, if permitted by the user's settings.

The types of data Google collects or stores may be different for users based on various settings the user has selected and what products they use. For example, if a user has signed in to their account and has "Web and App Activity" enabled, we may collect and store in the user's Account data about their activity on Google's services, like the user's search query and the URL they select on the Search results page. This can be helpful to users who wish to store this history; it also allows us to make better predictions about helpful results. If that user is not signed-in, however, we may still collect information about that query for use in some of our tools, like Google Trends (https://trends.google.com/), or to improve our products. We would not, however, associate that information with the user's Google account.

Additionally, Google has been a leader on data portability for over a decade, enabling our users to export their data and take it to another platform (for more information on this process and our recent improvements in this area, please see https://www.googblogs.com/author/markham-erickson/ and https://support.google.com/accounts/answer/3024190). Since 2011, Google has enabled users to easily move their content to competing services, with more than one billion gigabytes exported from Google products. This data download process, which we call Google Takeout, makes it possible for users to move their content to competing services, so no one feels they have to continue using Google if they prefer a service of another company (additional details are available at https://takeout.google.com/settings/takeout). This process can facilitate the export of data from more than 70 Google products, including Chrome, Gmail, Drive, Search, and YouTube. Users are able to export their data in a variety of industry standard formats that they can select based on product, type of data, and intended use. Users can also view a summary of the data saved in their Google accounts by following the instructions available at https://support.google.com/accounts/answer/162744. We know these features are being used - on average, we see 8.2 million exports per month with Google Takeout, and in 2021, more than 400 billion files were exported (a rate that has doubled since 2019).

Recognizing that data portability can be challenging for people who don't have high-speed internet, unlimited mobile data plans, or who don't have a personal device with extra storage, iIn 2018, we launched the Data Transfer Project (DTP), an open-source collaboration between Google, Apple, Meta, Microsoft, Twitter, and SmugMug to simplify data portability for people around the world. Unlike traditional methods of moving your files from one service to another, which require reliable broadband or drawing on mobile data plans, with DTP people can simply authorize a copy of the data to safely move to a new service without having to download it to a personal device first. (more information on this project is available at https://opensource.googleblog.com/2018/07/introducing-data-transfer-project.html and https://datatransferproject.dev/).

We recognize that privacy is not a one-size-fits-all proposition. Different users want to make different choices about how much information they share and how it is used. That is why we give our users control over their data privacy. To that end, we are continually focused on building tools that enable people to make the privacy choices that are right for them and their families.

Question 2. Ad-revenue used to support online piracy is a longstanding problem. Criminals profit by receiving advertising dollars in exchange for giving users free access to stolen movies, music, books, software, and other materials—stealing money from hardworking creators, including many small businesses and individual artists. A recent report found that over *a billion dollars a year* in advertising goes to supporting online pirated content.[1] Both the US and EU have been working on voluntary "follow the money" initiatives for several years with various actors, including Google, to stop funding theft. Yet the same report found that Google's advertising technologies provided 51 percent of ads to pirate apps.[2] This is particularly alarming given that other digital advertisers "almost never appear on piracy apps."[3]

a. **Why was Google identified as the top major brand involved in placing advertising on applications? What measures are you taking to change this?**

We share your interest in fighting online piracy and agree that one effective way to combat rogue sites that specialize in online piracy is to cut off their money supply. That is why we have worked diligently to block infringing sites and apps from using our services and work with other technology companies, publishers, and advertisers to develop and implement best practices for the advertising industry. These efforts have been successful. Around the world, online piracy has been decreasing, and spending on legitimate content is rising. Unfortunately, bad actors work hard to circumvent our systems and policies. While we recognize that we will never be able to fully eradicate piracy, we remain committed to these efforts and will continue to invest in our fight against piracy.

The report referenced in the question claims that advertisements of major brands are 24% of total ads on the reviewed applications. Of that 24%, advertisements for Google represented only 5% of those advertisements, which means that, according to the study, advertisements for Google were just 1.2% of the ads on the reviewed applications.

The report also notes that advertisements for major brands are 4% of total ads on the reviewed websites and that advertisements for Google were fewer than one percent of major

---

[1] Digital Citizens Alliance and White Bullet, Breaking (B)ads: How Advertiser-Supported Piracy Helps Fuel A Booming Multi-Billion Dollar Illegal Market (July 2021), https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf.
[2] *Id.*, pg. 34.
[3] *Id.*, pg. 17.

brand advertisements. This means advertisements for Google very rarely appeared on the reviewed websites.

It is also important to note that the methodology used in the report relies on a list of websites and apps that were identified by the author's own commercial machine-learning algorithm and includes data that is based on assumptions about ad revenue and traffic. Google is a leader in rooting out and ejecting rogue sites and apps from our publisher network. However, we acknowledge that no system is ever perfect and we remain committed to this work despite the challenges.

b. Does Google receive money from placing advertising on websites that contain pirated content?

We believe that one effective way to combat rogue sites that specialize in online piracy is to cut off their money supply. That is why we have been so committed to diligently blocking bad actors from using our services and helping set industry standards for safe online advertising. Our research has shown that AdSense ads, or ads that are matched with sites based on their content and visitors, appear on fewer than one-tenth of 1% of the pages that copyright owners identify in copyright removal notices for Search (more information on AdSense is available at https://support.google.com/adsense/answer/6242051).

c. What steps does Google take, both in the United States and worldwide, to prohibit advertising on piracy websites and applications?

We have always prohibited publishers from using our services to place ads on pages that contain pirated works, and we proactively monitor our network to root out bad publishers. In addition, when we receive a Digital Millennium Copyright Act (DMCA) notice for search, we take action to ensure that advertisements do not run on those same pages. Copyright holders can also notify us of pages or advertising that violates our policies through a webform.

We also work with other advertising leaders to craft best practices aimed at raising standards across the entire online advertising industry. Our efforts have been effective. In 2021, we blocked or removed 44.2 million advertisements that abused our policies related to copyright.

d. Do you agree that supporting commercial-scale pirate websites and apps through advertising dollars is wrong?

As noted above, we are and have been committed to diligently blocking bad actors from using our services and helping set industry standards for safe online advertising.

e. Does Google, or its agents or subsidiaries, block payment for ad impressions on pirated content?

We are always reviewing publisher pages for compliance with our policies. When we find ads running on pages that violate our policies, we remove the ads and stop the publisher from accruing further revenue on these pages.

f. **Does Google, or its agents or subsidiaries, conduct independent audits to ensure that any policies are being implemented effectively? How frequently are policies reviewed?**

We review our advertising policies and enforcement efforts regularly to ensure they remain up to date and effective. We have thousands of people globally working on policy development and enforcement. We actively track emerging trends and adversarial behavior and are quick to adapt our enforcement and policies accordingly. Additionally, in 2021, we added or updated over 30 policies for both advertisers and publishers.

We are active in industry associations that drive accountability through independent oversight on brand safety, operations, and reporting. YouTube was the first digital platform to ever receive accreditation from the Media Ratings Council's Enhanced Content Level Context and Brand Safety Guidelines, which are also sponsored by the American Association of Advertising Agencies, the Association of National Advertisers, and the Interactive Advertising Bureau. We also continue to work with the Global Alliance for Responsible Media on its strategic focus areas, such as exploring new reporting metrics on brand safety and improving brand safety tools across the industry to better manage advertising adjacency.

g. **Does Google collect data over its own ad placements that would allow it to prevent placement on websites or apps that pose a high risk for distributing illegal content, including pirated content?**

As detailed in our responses above, we currently use the most effective methods we can to prevent the placement of our own advertisements on websites and apps that contain potentially infringing content. We continue to examine ways that we can further improve.

h. **Google Ads is a tool offered to businesses and brands to place their ads in front of consumers. A brand chooses the type of audience it wants to reach and Google places the ad on the websites most likely to reach the target demographic. What steps are taken to ensure that ads are not placed on pirate websites?**

Please refer to our answer to Question 2c, above.

i. **What steps are taken to ensure that pirate publishers are prohibited from selling ad space through Google's advertising subsidiaries?**

Please refer to our answer to Question 2c, above.

j. What steps is Google taking to enhance transparency of its activities on its advertising networks?

We provide information about our policies and practices through our Google Transparency Report (available at https://transparencyreport.google.com/) and our Annual Ads Safety Report (available at https://blog.google/products/ads-commerce/ads-safety-report-2021/). We are committed to giving our users transparency, choice, and control when it comes to the ads they see on our platforms. We are working toward verification of all advertisers globally, and we recently announced that we are enhancing ad disclosures in the U.S. to link to advertiser pages that include an ad creative repository, the legal name, and country of origin for the advertiser.

Question 3. You stated in your testimony that Google does not sell data that it collects online.

a. Does Google share data collected in one business unit with other business units?

b. Does it share data collected with any legal entities outside of Google?

c. Does it share any of this data in connection with a legal business transaction?

At Google, we believe that data should be used to make consumers' lives better by improving the quality and diversity of products and services available, while protecting users' privacy and giving them control. Our business relies on earning our users' trust, specifically in how we use and protect their data. We work to maintain that trust by offering industry-leading controls to manage privacy. Three billion users visit their Google accounts every year, where they can review and change their privacy settings and delete data stored with their account.

Google does not sell users' personal information to anyone. That is not our business model, and we have always made this a touchstone of Google's relationship with our users. Google shares personal information with partners in the specific circumstances described in our Privacy Policy section on Google partners at https://policies.google.com/privacy/google-partners, including:

- With user consent: For example, if users use Google Home to make a reservation through a booking service, we will get their permission before sharing their name or phone number with the restaurant.
- For external processing: We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support.

- For legal reasons, such as to meet any applicable law, regulation, legal process, or enforceable governmental request.

In addition, our Privacy Policy (available at https://policies.google.com/privacy?hl=en-US) describes for users how we may use or combine data across our products, as well as the controls they have over their information. For example, depending on their settings, if a user watches videos of guitar players on YouTube, they might see an ad for guitar lessons on a site that uses our ad products. Some other examples of how we combine the information we collect include:

- When users are signed in to their Google Account and search on Google, they can see search results from the public web, along with relevant information from the content they have in other Google products, like Gmail or Google Calendar. This can include things like the status of an upcoming flight, restaurant, and hotel reservations, or their photos.
- If users have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when our users start to type in their name. This feature makes it easier to share things with people they know.

Question 4. Ms. Slaiman advocates for "a digital regulator to comprehensively the policy questions surrounding digital platforms."

a. **Do you agree that this is necessary?**

b. **Given the many issues beyond privacy and competition that address and implicate digital policy—including cybersecurity, national security, consumer rights, free speech, and intellectual property concerns—what existing agency would be the best situated, in your view, to carry out this role?**

c. **Is it important to you that the regulator should be politically accountable?**

We recognize policymakers and regulators are working to protect privacy while also considering whether making more data available among competitors would increase competition. We are encouraged to see some privacy and competition regulators conferring more formally to contribute their relevant expertise to the important questions being considered, for example when a privacy-oriented practice is being evaluated in an antitrust context. We will continue to engage with policymakers and regulators, as well as other stakeholders, to support thoughtful regulation that encourages innovation and protects consumers. For example, we continue to publicly support federal privacy legislation in the United States (more information is available at https://blog.google/outreach-initiatives/public-policy/the-urgent-necessity-of-enacting-a-national-privacy-law/).

Senator Tillis
Questions for the Record
Big Data, Big Questions: Implications for Competition and Consumers
Mr. John Robb, Global Guerillas Report

Q: The term "data" can have multiple meanings, which can sometimes generate confusion in policy discussions. How would you define "data" and "big data", as used in your written testimony?

A: The difference between data and "big data" is scale.

Big data has far more volume, variety, and velocity than traditional data. This complexity changes the way insight is generated from it. Instead of seeking definitive answers (customers are buying x more than y), analysts look for patterns. Patterns that can be useful in spotting opportunities, detecting problems, and shaping solutions. Finding these patterns through intentional analysis, particularly patterns that aren't ephemeral, is very difficult.

Big data is particularly useful for training AIs (machine learning). There's a high correlation between the amount of data used to train an AI and the quality of the AI. AIs trained using big data naturally find unexpected patterns and contextual cues that are useful in solving the problem they are trying to solve.

Q: How would you define consumer and user data, specifically what would be included and excluded from these definitions?

A: Traditional consumer data is mostly static demographic data. How much do you make, where do you live, and what is your education level?

That's radically changed with the arrival of networked user data. This new user data includes;

- Tracking data. Mouse and keyboard clicks. Page and site visits (on a single site and across sites). Physical location. Tracking over time and space. This is now expanding into detecting focus (eyeball tracking), physical measurement (health monitoring to hand movement), sensor data (pictures, videos, and other data collected by sensors in the environment, from a Tesla car to CCTV), etc.

- User-produced data. What people upload (both intentionally and unintentionally). Textual content (texting, blog posts, essays), voice content (podcasts to audio capture from Alexa or an iPhone), images (smartphone pictures to YouTube uploads). This data set is expanding.

- AI-training data (user-produced + tracking data at scale). User data is being used to actively train AIs. For example; Tesla uses user feedback and

> experiences to improve their self-driving system. Enlisting customers to actively train AIs is something we will see much more of in the future. Other firms strip mine the open Web (without consent) to build AIs (GPT-4 (text), Stable Diffusion (images), Google translate (text), etc.).

Q: Would this include user-uploaded videos, images, and text?

A: Yes, see above.

Q: Would such content be considered part of the "user" data, even if it includes content that originates from other sources?

A: Tracking data and uploaded data are both "user data." Data brokers aggregate this data for sale to marketing departments/firms and firms building AIs. Sometimes it is anonymized; sometimes, it isn't. Sometimes firms with access to user-tracking data sell it to generate extra revenue.

If the text or image being uploaded is from another source (somebody else took the picture or wrote the text), then it isn't user data, but the tracking data on the upload is. This is why the best approach to compensating people for data use is made in aggregate, at the population scale.

For example, a data ownership bill for the people of North Carolina would aggregate the data provided by people in the state. Data brokers, with a fiduciary duty to the people contributing to the data set, would compete to sign up people attached to this pool.

Data brokers representing individuals would solve the privacy problem in a way that doesn't destroy data (like in Europe). Data brokers, fueled by industry revenue, would have the lawyers and technologists needed to protect data and find new data sources collected by advancing technology. In contrast, privacy-based regulations rely on getting the attention of overwhelmed bureaucrats.

Q: Does it include data in which intellectual property rights, including copyright, trade secret, trademark, or design rights, may subsist?

A: No. There is already an industry that protects that data. However, firms that claim (like many social networks) all of the user-uploaded data and data collected about them, would not be allowed to claim ownership over it. That data would be owned by the individuals in question.

Q: How would you differentiate your proposal for people to own data from existing intellectual property rights-based approaches?

A: Technology has outpaced our laws. The data being generated by individuals isn't adequately protected by existing legal frameworks. Providing a mechanism for protecting the ownership rights of individuals in aggregate is critical to safeguarding against abuse (by corporations and the government) as well as providing a mechanism for participating in the AI-driven economy of the future.

To be precise: the data being strip-mined right now is being used to create the most valuable technological artifacts that have ever existed, without compensation to the people it is coming from. Making it possible for people to participate in the upside potential of this development will be as important as land ownership was to the development of capitalism (one of the most revolutionary aspects of the American Revolution, and why it was so important to early capitalism, was the ability of individuals without a hereditary title to own land).

Q: You advocate for a new form of digital identity. Could you please explain further what you mean by this, and how you envision it working in the current environment? Are there particular technologies that would need to be developed for this to be implemented?

A: Digital identity is necessary for the assignment of rights (of speech, ownership, etc.). It simply connects an online identity (collection of accounts, activities, etc.) to a living, breathing person in the physical world. Typically, this is done using the same approaches used for registering a financial account (government ID, etc.). It can become more sophisticated through the application of AI (as we are about to see with Twitter).

Q: Ms. Slaiman advocates for "a digital regulator to comprehensively the policy questions surrounding digital platforms." Do you agree that this is necessary?

A: If the digital regulator is overseeing the launch and establishment of a new industry (data brokers, etc.) and the technology standards that support it, then yes. If its intent is to build a regulatory enforcement body that is focused on privacy regulations and increasingly restrictive content moderation (as we see in the EU), then no. That would be a disaster (for example: China would win the AI race and the US and EU would suffer economic impoverishment due to it).

Q: Given the many issues beyond privacy and competition that address and implicate digital policy—including cybersecurity, national security, consumer rights, free speech, and intellectual property concerns—what existing agency would be the best situated, in your view, to carry out this role?

A: Something that looks like a cross between the SEC and Consumer protection. It would need to be focused on the individual, and their rights, while being able to manage the needs of growing a new industry (data brokers that represent the data pools that individuals join). This industry has the potential to rival finance

in size over time (percentage ownership or royalty rights from big AIs could be worth tens of trillions in the not-too-distant future).

Q: Is it important to you that the regulator should be politically accountable?

A: Of course. However, if the political focus is on the micromanagement of user data collection to shape society, then no. The goal of political discussions on this issue should be focused on creating the *minimum* viable rule set for a prosperous and successful society.

Senator Blackburn
Questions for the Record to John Robb
The Global Guerrillas Report

Q: It's imperative for the U.S. to get a national consumer privacy law in place—the EU and China have already done so. Given consumer concerns about how their data is being used online, what should that regime look like? What are the obstacles the United States faces in getting to that point?

A: There are three systems in place:

1. EU privacy laws use aggressive regulatory oversight to limit and destroy data.
2. China assigns ownership of data rights to the government and assigns loyal corporations the right to fully gather and exploit it.
3. US doesn't have a centralized approach. With few exceptions, it lets corporations do whatever they want in regard to data collection and exploitation.

Here's how this will play out:

- The EU approach is that it will prevent the development of the AIs and products/services that will drive economic growth in the future. Their approach to data is likely to result in economic impoverishment long term.

- The Chinese approach will generate economic growth and success. However, it will also be used for networked authoritarianism by the Chinese government. It will provide the government with complete control over the entire population in real time. From behavior to perception (through control of augmented reality).

- The US approach will yield some economic success, but it will be a system completely controlled by big corporations and a few wealthy individuals. Almost all of the economic success generated by this approach will concentrate in the hands of the corporations. Furthermore, the control

corporations have over data will allow them to dominate politics (in short, corporate-run network authoritarianism).

The solution?

The solution that allows the US the ability to succeed economically and avoid authoritarianism is to provide people with digital rights and data ownership. That approach would create an industry response to user data (an industry of data brokers/banks, much like the financial industry, which has a fiduciary responsibility to protect this data and maximize its returns). It ensures that the data needed to fuel development is available to corporations while allowing the people who provide this data a means of participating in the great wealth created by it.

Senator Chuck E. Grassley
Questions for Mr. John Robb:

Q: How important is the amount of data that a company has to their ability to effectively monetize that information?

A: A few thoughts on this:

- Data is key to success in a networked economy.
- The more you have and the better its quality, the more success you will have. NOTE: there is a high correlation between the amount of data you have available for an AI to train with and the quality of the AI.
- At the level of the economy, if corporations don't have access to data, they won't be able to match the products available from China that do have access.

Q: How difficult can it be for a startup or small business to collect enough data to be able to compete with companies that have large amounts of data?

A: It's hard, but it becomes impossible if the big companies control the small company's access to data. Big companies are using access to data as a weapon against the competition and as a means of extracting monopoly rents from their platforms. Apple and Google are good examples of this. This is already bad in the smartphone industry, it is going to become a catastrophe when augmented reality arrives (soon).

Q: Some commentators argue that the amount of data currently possessed by large incumbent companies forecloses the ability of new entrants to compete.

But, new data is being created every day and what data is important in the future may not be what is being collected today. If so, why isn't there an opportunity for additional companies to enter the market?

A: I agree. Data aggregation and privacy regulations (or "concerns') are being used by big companies to dominate marketplaces. New data is created, but these companies control the flow. For example, this control has allowed big companies in the smartphone market to charge a ~30% tax on transactions in the smartphone economy. It's extortionate.

Q: There is debate over whether Big Data should be regulated through the lens of consumer protection and privacy or whether antitrust laws should be used to address competition concerns with the collection of data. Do you have an opinion about the best approach to address this issue or should we be looking at a combination of different approaches?

Best approach: Data ownership for individuals. They contribute all of the data collected about them to big pools. These pools are managed by data brokers who have a fiduciary duty to protect this data and maximize the returns generated by it.

The data relationship between an app running on a smartphone or an augmented reality headset would be with the data brokers representing the individuals using the device. The device company wouldn't be able to use its control over data to extort monopoly rents. Instead, that benefit would flow to the individuals who contributed the data, providing them participation in the economy being built on this data.

A combo of SEC/banking (industry focus) and consumer protection agency would work best. The goal would be to set up a data brokerage/banking industry (with the individual as the client) that is so profitable that it could hire the people needed to enforce it.

February 21, 2023

The Honorable Richard J. Durbin
Chairman
Committee on the Judiciary
United States Senate
711 Hart Senate Building
Washington, D.C. 20510

Dear Chairman Durbin:

Thank you for the questions for the record from the Senate Committee on the Judiciary, Subcommittee on Competition Policy, Antitrust, and Consumer Rights hearing entitled "Big Data, Big Questions: Implications for Competition and Consumers," held on September 21, 2021. Per your request, attached are answers for the record to your questions.

Sincerely,

Meta Platforms, Inc.

575 7th STREET NW
STE 700
WASHINGTON, D.C. 20004

Meta

Senator Marsha Blackburn
Questions for the Record to Steve Satterfield, Vice President of Privacy & Public Policy, Facebook

1. **Please identify three distinct changes you have made to your platform to make it a safer and healthier experience for children.**

At Instagram, we have been working for a long time to help provide age-appropriate experiences on our platform; as part of that work, we recently announced some new tools and features to support keeping young people even safer on Instagram. Although we have made a number of changes, here are three recent examples:

Parental Tools. We launched tools in March 2022 to help parents and guardians guide and support their teens on Instagram. They can ask teens to enable them to view how much time their teens spend on Instagram and set time limits. We've also given teens the option to notify their parents if they report someone, giving their parents the opportunity to talk about it with them. These tools are available in our new Family Center. We worked closely with experts, parents, guardians and teens to develop Family Center, a place for parents and teens to work together on their accounts within Meta technologies, set up and use supervision tools, and access resources on how to communicate with their teens about internet use. This is just one step on a longer path—our vision for Family Center is to eventually allow parents and guardians to help their teens manage experiences across Meta technologies, all from one central place.

Family Center includes an education hub where parents and guardians can access resources from experts and review helpful articles, videos and tips on topics like how to talk to teens about social media. Parents can also watch video tutorials on how to use the supervision tools available on Instagram today. We worked closely with groups like Connect Safely and Net Family News to develop these resources, and we'll continue to add new information to Family Center's education hub. These parental supervision tools on Instagram allow parents and guardians to send invitations to their teens to initiate supervision tools, which enable them to:

- View how much time their teens spend on Instagram and set time limits;
- Set specific times during the day or week to limit their teen's use of Instagram;
- View what accounts their teens follow and the accounts that follow them;
- See more information when their teen reports an account or post, including who was reported, and the type of report;
- See a list of the accounts their teen is currently blocking on Instagram. The block list is in order of recency and denotes any users that have been blocked in the last seven days by the teen;
- See the teen's account settings specific to: (1) account privacy (public / private); (2) who can send the teen message requests (anyone / followers / no one); (3) who can add the

teen to a messaging group (everyone / only people they follow on Instagram); and (4) sensitive content controls (less / standard).

Additionally, in November 2022, we introduced updates on Facebook and Instagram to help further protect teens from online harm. For example, everyone who is under the age of 16 (or under 18 in certain countries) is now defaulted into more private settings when they join Facebook (a change we announced for Instagram in July 2021), and we encourage teens already on the app to choose these more private settings. We are also working with the National Center for Missing and Exploited Children to build a global platform for teens who are worried intimate images they created might be shared on public online platforms without their consent. This platform will be similar to work we have done to prevent the non-consensual sharing of intimate images for adults. It will allow us to help prevent a teen's intimate images from being posted online and can be used by other companies across the tech industry. In addition, we are working with Thorn and their NoFiltr brand to create educational materials that reduce the shame and stigma surrounding intimate images and empower teens to seek help and take back control if they've shared them or are experiencing sextortion.

Take A Break. We also launched "Take A Break" in certain countries to empower people to make informed decisions about how they're spending their time. If someone has been scrolling for a certain amount of time, we ask them to take a break from Instagram and suggest that they set reminders to take more breaks in the future. We show them expert-backed tips to help them reflect and reset. To make sure that teens are aware of this feature, we show them notifications suggesting they turn these reminders on.

Nudging Teens Towards Different Topics if They've Been Dwelling on One Topic for a While. Our research shows—and external experts agree—that if people are dwelling on one topic for a while, it could be helpful to nudge them towards other topics at the right moment. That's why we built an experience that will nudge people towards other topics if they've been dwelling on one topic for a while. This nudge is designed to encourage teens to discover something new and excludes certain topics that may be associated with appearance comparison.

We designed this feature because research suggests that nudges can be effective for helping people—especially teens — be more mindful of how they're using social media in the moment. In an external study on the effects of nudges on social media use, 58.2% of respondents agreed or strongly agreed that nudges made their social media experience better by helping them become more mindful of their time on-platform. Our own research shows they're working too: during a one-week testing period, one in five teens who saw our new nudges switched to a different topic.

In addition to this work, we continue to develop ways for people to verify their age on Instagram, allowing us to provide age-appropriate experiences. For example, in June 2022, we began testing new options for people on Instagram to verify their age, starting with people based in the US. If someone attempts to edit their date of birth on Instagram from under the age of 18 to 18 or over, we'll require them to verify their age using options such as uploading their ID or recording a video selfie. We're testing this so we can make sure teens and adults are in the right experience for their

age group. We are also partnering with Yoti, a company that specializes in online age verification, to help ensure people's privacy.

Our age verification tests show that our tools are working to help keep people within age-appropriate experiences. Since we began these new tools on Instagram, we've found that approximately four times as many people were more likely to complete our age verification requirements (when attempting to edit their date of birth from under 18 to over 18), equating to hundreds of thousands of people being placed in experiences appropriate for their age. We also were able to stop 96% of the teens who attempted to edit their birthdays from under 18 to 18 or over on Instagram from doing so. And we have found that 81% of people presented with our menu of options chose to use Yoti's video selfie to verify their age.

Senator Chuck E. Grassley
Questions for the Record to Mr. Steve Satterfield, Vice President, Privacy & Public Policy, Facebook

1. **Facebook monetize user's data by selling targeted advertisements. In the second quarter of 2021 Facebook had revenues of $29.08 billion. It has also been reported that the average American's data was worth $164 per year to Facebook. Is it accurate that the average America's data is worth $164 per year to Facebook?**

We publicly report our Average Revenue per User ("ARPU") on Facebook, both for advertising and other revenue, broken out by geographic region. ARPU is a revenue-based metric and not a valuation of people's data. As stated in our public financial filings, we define ARPU as our total revenue in a given geography during a given quarter, divided by the average of the number of monthly active users in the geography at the beginning and end of the quarter. In the U.S. and Canada, Facebook's ARPU from advertising was $58.77 in the fourth quarter of 2022.

We also report the Average Revenue per Person ("ARPP") across Meta's family of apps, both for advertising and other revenue. As with ARPU, ARPP is a revenue-based metric and not a valuation of people's data. As stated in our public financial filings, we define ARPP as our total revenue during a given quarter, divided by the average of the number of MAP at the beginning and end of the quarter. Meta's ARPP from advertising across its family of apps was $8.63 in the third quarter of 2022.

For more information, please see our latest earnings presentation (https://s21.q4cdn.com/399680738/files/doc_financials/2022/q4/Earnings-Presentation-Q4-2022.pdf).

2. **There is debate over whether Big Data should be regulated through the lens of consumer protection and privacy or whether antitrust laws should be used to address competition concerns with the collection of data. Do you have an opinion about the best approach to address this issue or should we be looking at a combination of different approaches?**

Meta has long called for regulation in the digital space on issues like privacy and data security, combating foreign election interference, content moderation, and data portability. The issues facing the industry are complex, multi-faceted, and impact peoples' lives. Accordingly, Meta is committed to working with policymakers to craft the right regulations. Meta is amenable to reviewing proposed legislation and providing comments.

More information about our approach to regulation can be found here: https://about.meta.com/regulations/?utm_source=about.facebook.com&utm_medium=redirect.

Senator Josh Hawley
Questions for the Record to Steve Satterfield, Vice President of Privacy & Public Policy, Facebook

1. **Please provide copies of all research findings or reports, whitepapers, slideshows, meeting recordings, or other documentation circulated within Facebook, over the past ten years, pertaining to each of the following topic areas:**

   a) **Addiction or addictive behaviors associated with the use of Facebook's products and services;**
   b) **Depression and/or self-harm associated with the use of Facebook's products and services;**
   c) **Impact of Facebook's products and services on the mental health and wellness of users under age 18;**
   d) **Extent to which Facebook's products and services are accessed by users under age 13**
   e) **Development of novel products or services targeted specifically to users under age 13.**

We want social media to be a positive force in teens' lives, so we're listening to feedback from experts and our community to build apps where teens can discover and create in an age-appropriate way; as part of that work, we have developed tools and features to support keeping young people even safer on Instagram. For example:

Parental Tools. We are committed to working with parents and families, as well as experts in child development, online safety, and children's health and media, to ensure we are building appropriate tools and features for families. That means building tools that promote meaningful interactions and helping people manage their time on our platform. It also means providing information, resources, and tools for parents and teens to work together to develop healthy and safe online habits. And it means continued learning in this area.

We believe that parents and guardians know what is best for their teens, and we've developed more than 30 tools to support teens and families, including developing supervision tools that allow parents and guardians to ask teens to enable them to be more involved in their teens' experiences. In March 2022, we rolled out supervision tools that allow parents and guardians to: (1) view how much time their teens spend on Instagram and set time limits; (2) be notified when their teen shares they've reported someone; and (3) view and receive updates on what accounts their teens follow and the accounts that follow their teens. In June 2022, we introduced additional features that allow parents and guardians to send invitations to their teens to initiate supervision tools, set specific times when they would like to limit their teen's use of Instagram, and see more information when their teen reports an account or post, including who was reported, and the type of report. We make video tutorials on how to use these supervision tools available for parents and guardians in the Family Center's education hub.

Additionally, in November 2022, we introduced updates on Facebook and Instagram to help further protect teens from online harm. For example, everyone who is under the age of 16 (or

under 18 in certain countries) is now defaulted into more private settings when they join Facebook (a change we announced for Instagram in July 2021), and we encourage teens already on the app to choose these more private settings. We are also working with the National Center for Missing and Exploited Children to build a global platform for teens who are worried intimate images they created might be shared on public online platforms without their consent. This platform will be similar to work we have done to prevent the non-consensual sharing of intimate images for adults. It will allow us to help prevent a teen's intimate images from being posted online and can be used by other companies across the tech industry. In addition, we are working with Thorn and their NoFiltr brand to create educational materials that reduce the shame and stigma surrounding intimate images, and empower teens to seek help and take back control if they've shared them or are experiencing sextortion.

Take A Break. We also launched "Take A Break" in certain countries to empower people to make informed decisions about how they're spending their time. If someone has been scrolling for a certain amount of time, we ask them to take a break from Instagram and suggest that they set reminders to take more breaks in the future. We also show them expert-backed tips to help them reflect and reset. To make sure that teens are aware of this feature, we show them notifications suggesting they turn these reminders on.

Nudging Teens Towards Different Topics if They've Been Dwelling on One Topic for a While. Our research shows—and external experts agree—that if people are dwelling on one topic for a while, it could be helpful to nudge them towards other topics at the right moment. That's why we built an experience that will nudge people towards other topics if they've been dwelling on one topic for a while. This nudge is designed to encourage teens to discover something new and excludes certain topics that may be associated with appearance comparison.

We designed this feature because research suggests that nudges can be effective for helping people — especially teens — be more mindful of how they're using social media in the moment. In an external study on the effects of nudges on social media use, 58.2% of respondents agreed or strongly agreed that nudges made their social media experience better by helping them become more mindful of their time on-platform. Our own research shows they're working too: during a one-week testing period, one in five teens who saw our new nudges switched to a different topic.

In addition to this work, we prohibit people under the age of 13 from using Facebook and Instagram, and when we learn that someone under 13 years old is on our platform, we remove them. We also continue to develop ways for people to verify their age on Instagram, allowing us to provide age-appropriate experiences. For example, in June 2022, we began testing new options for people on Instagram to verify their age, starting with people based in the US. If someone attempts to edit their date of birth on Instagram from under the age of 18 to 18 or over, we'll require them to verify their age using options such as uploading their ID or recording a video selfie. We're testing this so we can make sure teens and adults are in the right experience for their age group. We are also partnering with Yoti, a company that specializes in online age verification, to help ensure people's privacy.

Our age verification tests show that our tools are working to help keep people within age-appropriate experiences. Since we began these new tools on Instagram, we've found that approximately four times as many people were more likely to complete our age verification requirements (when attempting to edit their date of birth from under 18 to over 18), equating to hundreds of thousands of people being placed in experiences appropriate for their age. We also were able to stop 96% of the teens who attempted to edit their birthdays from under 18 to 18 or over on Instagram from doing so. And we have found that 81% of people presented with our menu of options chose to use Yoti's video selfie to verify their age.

Meta conducts research on these important issues to understand how people experience its apps. We use our research to inform changes to our apps and provide resources for the people who use them. We are committed to learning even more about issues related to well-being, and we welcome the opportunity to work with Congress and others in the industry on this important topic.

We offer researchers a number of privacy-protective methods to collect and analyze data. We welcome research that challenges us to innovate and that doesn't compromise the security of our platform or the privacy of the people who use it. Meta researchers have also published and shared hundreds of papers, and we will continue to work to publish research externally and to engage and collaborate with experts, including in data-sharing with researchers on issues related to young people. For more information about research we make available, please visit https://research.facebook.com/.

Finally, in December 2022, we held our first Meta Summit focused on Youth Safety and Well-Being to discuss this work. Safety advocates, mental health experts, educators, think tank researchers, policy writers and parents—many of whom helped inform the development of these tools—gathered in Washington, D.C. to discuss challenges families face in the digital age and explore opportunities to better serve teens and families. At the Summit, Nick Clegg, Meta's President of Global Affairs, called for global policymakers and regulators to work together on clear, consistent regulation when it comes to providing safe, age-appropriate experiences for young people online. We support regulators across the globe working together to establish clear, consistent laws that adapt to ever-evolving technologies, so they can be implemented successfully by companies across our industry. We're hopeful that continued regulation in this area will seek to preserve teens' rights to be online, while creating safe, supportive environments for them to express themselves.

2. **Please provide the following information:**

   a) **How much revenue, in the aggregate, does Facebook estimate that it makes from users under 18?**
   b) **How much revenue does Facebook estimate that it makes from *each individual* user under 18?**
   c) **How much revenue, in the aggregate, does Facebook estimate that it makes from users under 13?**
   d) **How much revenue does Facebook estimate that it makes from *each individual* user under 13?**

We publicly report our Average Revenue per User ("ARPU") on Facebook, both for advertising and other revenue, broken out by geographic region. In the US and Canada, Facebook's ARPU from advertising was $58.77 in the fourth quarter of 2022. We also report the Average Revenue per Person ("ARPP") across Meta's family of apps, both for advertising and other revenue. Meta's ARPP from advertising across its family of apps was $8.63 in the fourth quarter of 2022. For more information, please see our latest earnings presentation (https://s21.q4cdn.com/399680738/files/doc_financials/2022/q4/Earnings-Presentation-Q4-2022.pdf). We do not break out this information publicly by age. We prohibit people under the age of 13 from using Facebook and Instagram, and when we learn that someone under 13 years old is on our platform, we remove them.

3. **On September 27, Instagram head Adam Mosseri announced that the company was pausing efforts "to build an Instagram experience for people under the age of 13, often referred to as 'Instagram Kids,'" but "[stood] by the need to develop this experience" and intended "to work with parents, experts, policymakers and regulators, to listen to their concerns, and to demonstrate the value and importance of this project for younger teens online today."**

   a) **When, if at all, does Facebook project that it will resume development on "an Instagram experience for people under the age of 13"?**
   b) **On the basis of what considerations did Facebook conclude that it was more important to develop a designated digital space for users under 13 than, conversely, to ramp up efforts to prevent use of the platform by these users altogether?**

We started work to build an Instagram experience for tweens (aged 10-12) to address an issue seen across our industry: tweens are getting phones younger and younger, misrepresenting their age, and downloading apps that are meant for those 13 or older. This is an industry-wide concern, and other tech companies have built experiences for tweens. For example, YouTube and TikTok both have versions of their apps built specifically for those under 13. Additionally, we launched Messenger Kids in 2017 after meeting with thousands of parents, parenting organizations, child safety advocates and child development experts about the need for a messaging app that lets kids have fun connecting with friends and family while giving parents control over the experience.

The Instagram experience for tweens was intended to focus on delivering age-appropriate experiences and provide parents and guardians visibility and control over what their tweens are doing online. While we stand by the need to develop this Instagram experience, in September 2021, we announced that we were pausing this work. To be clear, our intention was not for this version to be the same as Instagram today. It was never meant for younger kids, but for tweens (aged 10-12). It would have required parental permission to join, we would not have shown ads, and it would have had age-appropriate content and features. Parents would have been able to supervise the time their tweens spent on the app and oversee who could message them, who could follow them, and whom they could follow.

We also continue to build technology to find and remove Instagram accounts belonging to people under the age of 13. We have tools and processes to identify and remove people who falsely state

they are 13 years old or older. For example, anyone can report an underage account to us. Our content reviewers are also trained to flag reported accounts that appear to be used by people who are underage. If these people are unable to prove they meet our minimum age requirements, we delete their accounts. In the last two quarters of 2021, Meta removed more than 4.8 million accounts on Facebook and 1.7 million accounts on Instagram because they were unable to meet our minimum age requirement.

Senator Thom Tillis
Questions for the Record to Steve Satterfield, Vice President of Privacy & Public Policy, Facebook

1. **The term "data" can have multiple meanings, which can sometimes generate confusion in policy discussions. How would you define "data" and "big data", as used in your written testimony?**
    a. **How would you define consumer and user data, specifically what would be included and excluded from these definitions?**
    b. **Would this include user uploaded videos, images, and text?**
    c. **Would such content be considered part of the "user" data, even if it includes content that originates from other sources?**
    d. **Does it include data iu which intellectual property rights, including copyright, trade secret, trademark, or design rights, may subsist?**

As explained in our Privacy Policy, we collect four basic categories of data about people: (1) data about their activity and information they provide; (2) data about their friends, followers, and other connections; (3) data about their app, browser and devices; and (4) data we receive from partners, vendors and third parties, including the websites and apps that use our business tools. Our Privacy Policy provides more detail about each of the four categories.

People retain ownership of the intellectual property rights (things like copyright or trademarks) in any such content that they create and share on our platforms. Nothing in our Terms of Service takes away the rights people have to their own content, and they are free to share their content with anyone else, wherever they want.

As far as the amount of data we collect about people, the answer depends on the person. People who have only recently signed up for Facebook have usually shared only a few things—such as name, contact information, age, and gender. Over time, as people use our products and interact with our services, we receive more data from them, and this data helps us provide more relevant content and services. That data will fall into the categories noted above, but the specific data we receive will, in large part, depend on how the person chooses to use Facebook. For example, some people use Facebook to share photos, so we receive and store photos for those people. Some people enjoy watching videos on Facebook; when they do, we receive information about the video they watched, and we can use that information to help show other videos in their Feeds. Other people seldom or never watch videos, so we do not receive the same kind of information from them, and their Feeds are likely to feature fewer videos.

The data we have about people also depends on how they have used our controls. For example, people who share photos can easily delete those photos. The same is true of any other kind of content that people post on our services. Through Facebook's Activity Log tool, people can also control information about their engagement—i.e., their likes, shares, and comments— with other people's posts. The use of these controls affects the data we have about people.

We also offer a variety of tools to help users understand the data Facebook has about them. These include the Access Your Information and Download Your Information tools available to people

who use Facebook in their account settings. And to provide more transparency and control around these practices, Off-Facebook Activity lets people see a summary of apps and websites that send us information about their activity and allows them to disconnect this information from their account if they choose. For more information about this tool, please see our Help Center.

2. **Ad-revenue used to support online piracy is a longstanding problem. Criminals profit by receiving advertising dollars in exchange for giving users free access to stolen movies, music, books, software, and other materials—stealing money from hardworking creators, including many small businesses and individual artists. A recent report found that over *a billion dollars a year* in advertising goes to supporting online pirated content.[1] Both the US and EU have been working on voluntary "follow the money" initiatives for several years with various actors, including Facebook, to stop funding theft. Yet the same report found that Facebook was a top ad spender, accounting for 27% of major brand advertising appearing on piracy apps.[2] This is particularly alarming given that other digital advertisers "almost never appear on piracy apps."[3]**

    a. **What steps does Facebook take, both in the United States and worldwide, to prohibit advertising on piracy websites and applications?**
    b. **Why was Facebook identified as the top major brands involved in placing advertising on applications? What measures is Facebook taking to change this?**
    c. **Does Facebook agree that supporting commercial-scale pirate websites and apps through advertising dollars is wrong?**
    d. **Does Facebook, or its agents or subsidiaries, identify websites or apps that pose a risk of distributing or displaying copyright protected content without authorization?**
    e. **Does Facebook, or its agents or subsidiaries, restrict the display of its advertisements on websites that infringe copyright, or pose a high risk of engaging in copyright infringement?**
    f. **Does Facebook, or its agents or subsidiaries, block payment for ad impressions on pirated content?**
    g. **Does Facebook, or its agents or subsidiaries, conduct independent audits to ensure that any policies are being implemented effectively? How frequently are policies reviewed?**
    h. **Does Facebook collect data over its own ad placements that would allow it to prevent placement on websites or apps that pose a high risk for distributing illegal content, including pirated content?**
    i. **What steps is Facebook taking to enhance transparency of its activities on its advertising networks?**

---

[1] Digital Citizens Alliance and White Bullet, *Breaking (B)ads: How Advertiser-Supported Piracy Helps Fuel A Booming Multi-Billion Dollar Illegal Market* (July 2021), https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf.
[2] *Id.*, pg. 17.
[3] *Id.*, pg. 17.

Facebook takes creativity, copyright, and protection of intellectual property rights seriously. We strongly oppose the placement of our advertisements on websites and apps that either infringe or pose a high risk of infringing copyright (including on commercial-scale pirate websites and apps). We maintain a robust framework to combat misplacement of Facebook ads on third-party websites and apps. Part of that work involves taking proactive steps to protect IP and combat piracy and the sale and promotion of counterfeit goods.

Advertisement Fraud Management Framework. The goal of our advertisement fraud management framework is two-fold: (i) to prevent fraudulent traffic sources from bidding on or serving Facebook ads; and (ii) to prevent payments for identified fraud traffic. To accomplish these goals, our general practice is to request third-party agencies with whom we contract to proactively identify and protect against fraudulent traffic.

Our current ad fraud management framework is divided into three activities: (1) prevention; (2) detection; and (3) mitigation:

1. **Prevention:** Fraud prevention begins during advertisement network selection. From this selection process, Facebook contracts with industry-leading third-party digital media agencies to place ads for our platforms and services on external websites and apps. Our general practice is to request direct, transparent placements, and request that fraud terms be included in our agreements. In negotiating these agreements, we generally request that vendors agree to actively monitor ad campaigns for signs of fraudulent activity, and agree to alert us in the event that any such activity is detected or suspected. Our general practice also includes that vendors agree to ensure that our ads do not appear adjacent to any content promoting subjects such as pornography, non-gaming violence, or infringement of intellectual property rights (including music and video piracy) or on websites that promote those activities. While each agreement is unique, the foregoing reflects some of the terms that we strive to obtain in our agreements with vendors.

2. **Detection:** We utilize tools and fraud suites from third-party agencies, such as the Kochava Fraud Console and tools from Forensiq and DoubleVerify, to try to detect fraudulent placements (including advertisements on websites that either infringe or pose a high risk of infringing copyright). We monitor these placements and try to identify any anomalies that may signal fraudulent or suspicious activity. We, in close collaboration with these third-party agencies, also develop custom, threshold-based signals to detect app and web traffic that leads to suspicious activity.

3. **Mitigation:** We maintain global blocklists intended to prevent our ads from appearing on apps and websites associated with fraud, fake actors, or sensitive content. Our partnership with third-party agencies allows us to permanently block identified fraudulent ad sources, such as websites and apps, and to identify potentially problematic traffic, which is flagged for investigation in partnership with the ad network/publisher. Since our November 2021 response to you on this topic, we have doubled down on the breadth of these efforts. We are now also working with industry stakeholders across the world to identify websites that may be dedicated to piracy or to facilitating copyright infringement. Once identified via our trusted sources, we use internal criteria to identify which URLs should be added to our

blocklists. Meta ads will not appear on any external URL that has been added to the blocklist—thereby significantly reducing any risk of funding or facilitating piracy on the Facebook platform. Further, our mitigation framework consists of utilizing automatic and manual blocking technology to investigate problematic traffic with ad networks. Finally, if any fraud or violations of the underlying agreement with the ad placement agency are identified, our practice is to request refunds for the ad impression. We recognize that no matter our preventative measures, there must always be ongoing manual traffic reviews to spot and investigate suspicious signals. As such, we regularly assess and continue to make improvements to our detection and protection framework, to improve our detection of ads that appear on or are attributed to fraud traffic sources.

Through partnership with third-party agencies, we strive to update our blocklists weekly. Additionally, these third-party agencies have advised us that they conduct regular audits (on the weekly and monthly level) to evaluate fraud safety measures. Managing our ad placements globally can be challenging and is an iterative process. For example, for one of the ads referenced in the Breaking (B)ads report, our teams determined that ten versions or variations of the piracy app already appeared on our permanent blocklist. Further, as a result of the information provided in the report, our teams added an additional four variations of the app to our permanent blocklist. As detailed above, we, in close partnership with third-party vendors, continue to proactively identify how we can improve in this area, and take steps to help protect current and non-users from seeing ads on inappropriate websites and apps, including on those that either infringe or pose a high risk of infringing copyright advertisements.

3. **Your written testimony states that there are "always risks when people transfer data online." Please elaborate on the nature and scope of these risks, and the people and entities who are implicated by these risks.**

    a. **What steps does Facebook take to inform others of these risks?**

Last year, we rewrote and re-designed our Privacy Policy to make it easier to understand and clearer about how we use people's information, and we updated our Terms of Service to better explain what is expected from us and those who use our platforms. The updates to our Privacy Policy include detailed explanations about how we use and share information with third parties. Also, our Help Center contains information and answers to frequently asked questions. When a user decides to login with Facebook or connect their account, we provide information about where they are sending the data, what that destination will receive, and access to that destination's privacy policy.

    b. **How does the Data Transfer Project address these risks?**

The open source Data Transfer Project is a collaborative effort by a group of companies, including Meta, to build a common framework with open-source code that can connect any two online services, enabling a seamless user-initiated portability of data between platforms. The Data Transfer Project's open-source framework powers our Transfer Your Information tool, which enables people to transfer their Facebook photos and videos, notes, posts, and events directly to destinations including BackBlaze, Dropbox, Koofr, Google Photos, Photobucket, Google Calendar, Google Docs, Blogger, and WordPress.

In 2018, the Data Transfer Project published a white paper describing the fundamentals of the project and its principles on a range of topics including privacy and security.

Neither the Data Transfer Project, nor any one company acting alone can resolve the challenging tradeoffs involving data portability like those we identified in our own 2019 white paper on data portability.

4. **Ms. Slaiman advocates for "a digital regulator to comprehensively the policy questions surrounding digital platforms."**
    a. **Do you agree that this is necessary?**
    b. **Given the many issues beyond privacy and competition that address and implicate digital policy—including cybersecurity, national security, consumer rights, free speech, and intellectual property concerns—what existing agency would be the best situated, in your view, to carry out this role?**
    c. **Is it important to you that the regulator should be politically accountable?**

We support updated regulations in the digital space on issues like privacy and data security, combating foreign election interference, content moderation, and data portability, and we have called for the US to create a new digital regulator. The issues facing the industry are complex, multi-faceted, and impact peoples' lives. Accordingly, Meta is committed to working with policymakers to craft the right regulations, and is amenable to reviewing proposed legislation and providing comments.

We have been open about our support for updated regulations on key issues. More information about our approach to regulation can be found here: https://about.meta.com/regulations/?utm_source=about.facebook.com&utm_medium=redirect.

Big Data, Big Questions: Implications for Competition and Consumers
September 21, 2021
Response to Questions for the Record
Charlotte Slaiman
Competition Policy Director
Public Knowledge
Washington, D.C.

Responses to Senator Grassley

1. **How important is the amount of data that a company has to their ability to effectively monetize that information?**

One of the important features of data as an economic good is that it exhibits increasing returns to both scope and scale. That means that more data is exponentially more valuable, particularly when it comes from different sources. This makes it incredibly difficult for a startup company with only one source of data to properly compete against Big Tech's massive data collection operation.

2. **How difficult can it be for a startup or small business to collect enough data to be able to compete with companies that have large amounts of data?**

It can be very difficult. Consumers might have less trust in a name or brand they do not recognize. An already established Big Tech titan can use their other sources of data on you to "fill in the gaps" in a way that a smaller business with just one or two products cannot, unless they purchase that data from an external source. This allows for a greater degree of targeting and other data exploitation by Big Tech firms.

3. **Some commentators argue that the amount of data currently possessed by large incumbent companies forecloses the ability of new entrants to compete. But, new data is being created every day and what data is important in the future may not be what is being collected today. If so, why isn't there an opportunity for additional companies to enter the market?**

There is still not a fair opportunity for additional companies to enter the market because of the powerful market position of the largest platforms, together with the lack of fair competition rules such as interoperability and non-discrimination requirements. This allows the largest platforms to continue their control of new data points and makes it much harder for competitors to enter.

I addressed this question further in my written testimony on page 7:

"The dominant platforms sometimes argue that data ages rapidly, so a new competitor could quickly amass the data needed to compete. This is theoretically true, but it is not just old data that today's dominant digital platforms control. Users are still today locked in to these platforms through their gatekeeper power, so the platforms continue to have access to ongoing data streams. These data streams can be used to continuously update algorithms to stay on top. They can also keep platforms updated about the users so as not to rely on just static or past data about them. This allows platforms to not just 'know' their users, but see how their users change over time—often in response to the algorithms that platforms created using older user data. This cycle of collection, use, and iteration gives platforms significant power over their users."

4. **There is debate over whether Big Data should be regulated through the lens of consumer protection and privacy or whether antitrust laws should be used to address competition concerns with the collection of data. Do you have an opinion about the best approach to address this issue or should we be looking at a combination of different approaches?**

I certainly believe that a combination of approaches is superior. Technology platforms present a myriad of issues for our society, and our solutions need to account for the interactions at play. Antitrust alone is not enough. There is a needed role for privacy, consumer protection, and civil rights. A privacy regime focused on data minimization and a more restrictive environment for the collection, spread, and use of consumer data would certainly help control for some of the advantages dominant platforms receive from their unchecked and pervasive collection of consumer data. Public Knowledge is supportive, for example, of bipartisan comprehensive privacy legislation that Congress is considering that would limit data collection practices of online platforms, data brokers, and others.

Consumers should not have to choose between competitive markets and their privacy. Congress must act to safeguard user privacy *and* to promote fair competition on and against the largest firms.

Responses to Senator Tillis

1. **The term "data" can have multiple meanings, which can sometimes generate confnsion in policy discussions. How wonld yon define "data" and "big data", as used in your written testimony?**

Your question gets at the complexity of the "data" definition in policy discussions. This can be a difficult question to answer and is perhaps why recent legislation (S. 2992, *The American Innovation and Choice Online Act*) calls for a Federal Trade Commission rulemaking to define "data." I would define "data" as anything a platform collects and uses to either monetize or improve its services. However, the term certainly can have multiple meanings, so it's important

that we continue to define what we mean by "data" in different contexts. "Big data" refers to data sets large enough to be useful for training machine learning algorithms and similar purposes. Big Tech platforms have a built-in advantage in collecting big data sets.

a. How would you define consumer and user data, specifically what would be included and excluded from these definitions? For example, the section of data portability refers to "your data" – what would this include?

When it comes to protecting user privacy, consumer and user data can be defined as information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual and may include derived data and unique identifiers. This could be things like your IP address, your mobile phone's device identifier, location data, or anything collected about your personal behavior online or when combined with information collected online is reasonably likely to identify an individual. In the context of data portability, the definition of "your data" would be different for different product categories based on what is needed to promote a competitive marketplace. Ongoing communication across social media networks requires interoperability of different categories of data than porting a customer over to a rival phone carrier, for example. Of course, since portability or interoperability should only be happening at the user's request, the user would also decide which data categories they actually want to transfer.

b. Would this include user uploaded videos, images, and text?

Yes, in general I would expect effective data portability requirements to include these items. This means companies would need to offer this option to consumers, and consumers could choose which of their videos, images, or text communications—if any—to transfer.

c. Would such content be considered part of the "user" data, even if it includes content that originates from other sources?

Yes. A user should be able to download material they have uploaded, even when that content originates from other sources. Uploaded material (for example, in the form of memes, reaction images, or even emoji) is as much a part of how many people communicate online as their own words. Failing to allow this material to be exported would hamper the goals of competition and interoperability.

d. Does it include data in which intellectual property rights, including copyright, trade secret, trademark, or design rights, may subsist?

Not necessarily. I would think that the important part of most user's data is their relationship to a copyrighted work, not necessarily the work itself. For example, my user data might include positive interactions with the movie "Mad Max: Fury Road"—posts I've liked about it, me posting about it, etc. However, that data would not implicate any sort of IP rights in the actual movie. In some cases, users may upload content (*e.g.*, memes or snippets of text) that are fair

uses of copyrighted material. In any event, data portability requirements do not provide new grounds for the infringement of IP rights.

2. **Your testimony advocates for "a digital regulator to comprehensively the policy questions surrounding digital platforms."**
    a. **Given the many issues beyond privacy and competition that address and implicate digital policy—including cybersecurity, national security, consumer rights, free speech, and intellectual property concerns—what existing agency would be the best situated, in your view, to carry out this role?**

There is no one agency today that is best suited to properly deal with the cross-cutting issues presented by technology platforms that your question identifies. That is why Public Knowledge advocates for a completely new agency. Both the Federal Trade Commission and the Federal Communications Commission have some tools and expertise in common with what a digital regulator would need—but either one would need additional authority, staffing, and budget to achieve the goals of a digital regulator.

    b. **Is it important to you that the regulator should be politically accountable?**

Political accountability is important and can foster trust in an agency's decisions. Public Knowledge has advocated for a bipartisan commission-like structure (similar to the Federal Trade Commission or the Federal Communications Commission) as the structure that strikes the right balance between political insulation and accountability.

3. **Your testimony refers to data portability as an important tool "to neutralize the power that Big Data confers upon dominant digital platforms."**
    a. **In your view, is the Data Transfer Project, described in Google's testimony as a partnership among Google, Apple, Facebook, Microsoft, and Smugmug, an acceptable way to address data portability?**

While projects like the Data Transfer Project are laudable, I believe they are insufficient to solve data portability and interoperability problems. Company commitments without agency enforcement only get you so far. Firms might not make some key data available and can cut off portability to rivals that pose a competitive threat. This is a key component of the ongoing Facebook FTC litigation. Facebook offered access to its network to companies that would increase engagement with the core Facebook product but cut off would-be rivals like Vine. I strongly believe we need federal legislation in this area in the vein of the bipartisan ACCESS Act.

○