UNDERSTANDING THE DIGITAL ADVERTISING ECOSYSTEM

HEARING

BEFORE THE

SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JUNE 14, 2018

Serial No. 115–139

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
34–638 PDF WASHINGTON : 2019

COMMITTEE ON ENERGY AND COMMERCE

GREG WALDEN, Oregon
Chairman

JOE BARTON, Texas
Vice Chairman
FRED UPTON, Michigan
JOHN SHIMKUS, Illinois
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota
TIM WALBERG, Michigan
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina

FRANK PALLONE, JR., New Jersey
Ranking Member
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan

SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION

ROBERT E. LATTA, Ohio
Chairman

ADAM KINZINGER, Illinois
Vice Chairman
FRED UPTON, Michigan
MICHAEL C. BURGESS, Texas
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
DAVID B. MCKINLEY, West Virgina
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
LARRY BUCSHON, Indiana
MARKWAYNE MULLIN, Oklahoma
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
JEFF DUNCAN, South Carolina
GREG WALDEN, Oregon *(ex officio)*

JANICE D. SCHAKOWSKY, Illinois
Ranking Member
BEN RAY LUJÁN, New Mexico
YVETTE D. CLARKE, New York
TONY CÁRDENAS, California
DEBBIE DINGELL, Michigan
DORIS O. MATSUI, California
PETER WELCH, Vermont
JOSEPH P. KENNEDY, III, Massachusetts
GENE GREEN, Texas
FRANK PALLONE, JR., New Jersey *(ex officio)*

C O N T E N T S

WITNESSES

SUBMITTED MATERIAL

[1] Mr. Zaneis did not answer submitted questions for the record by the time of printing.

[2] The information has been retained in committee files and also is available at *https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108413.*

UNDERSTANDING THE DIGITAL ADVERTISING ECOSYSTEM

THURSDAY, JUNE 14, 2018

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:16 a.m., in room 2322, Rayburn House Office Building, Hon. Robert Latta (chairman of the subcommittee) presiding.

Members present: Representatives Latta, Kinzinger, Burgess, Upton, Lance, Guthrie, Bilirakis, Bucshon, Walters, Costello, Schakowsky, Cárdenas, Dingell, Matsui, Welch, Kennedy, Green, and Pallone (ex officio).

Staff present: Melissa Froelich, Chief Counsel, Digital Commerce and Consumer Protection; Adam Fromm, Director of Outreach and Coalitions; Ali Fulling, Legislative Clerk, Oversight and Investigations, Digital Commerce and Consumer Protection; Elena Hernandez, Press Secretary; Paul Jackson, Professional Staff Member, Digital Commerce and Consumer Protection; Bijan Koohmaraie, Counsel, Digital Commerce and Consumer Protection; Mark Ratner, Policy Coordinator; Austin Stonebraker, Press Assistant; Greg Zerzan, Counsel, Digital Commerce and Consumer Protection; Michelle Ash, Minority Chief Counsel, Digital Commerce and Consumer Protection; Jeff Carroll, Minority Staff Director; Lisa Goldman, Minority Counsel; Carolyn Hann, Minority FTC Detailee; Caroline Paris-Behr, Minority Policy Analyst; and C.J. Young, Minority Press Secretary.

Mr. LATTA. Well, good morning, and welcome to the Subcommittee on Digital Commerce and Consumer Protection. We really appreciate you all being here, and we look forward today to your testimony.

And at this time, I'll recognize myself for 5 minutes for an opening statement. And again, good morning and I wanted to again thank our witnesses for being with us today.

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

An advertisement used to mean a quarter-page section in your local newspaper, a billboard along the highway, or as our chairman of the full committee would know in his radio days, a radio spot during the rush-hour commute.

While those types of advertisements still exist, targeted digital advertising has begun to dominate the advertising and marketing industry.

The digital advertising ecosystem is complex and often misunderstood. Today, we hope to clear up some of this confusion for consumers and discuss both the benefits and emerging, often high-profile, challenges of online advertising.

Our expert panel of witnesses will explain how this technology works and its place in our economy and our lives.

According to the Interactive Advertising Bureau, the ad-supported internet ecosystem generated over $1 trillion for the U.S. economy in 2016 and was responsible for 10.4 million jobs with 44 percent of those jobs employed by small and medium businesses.

The massive growth of online advertising's contribution to GDP can be tied to improved data collection and subsequent ad targeting. Digital ads are dependent on consumer-related information and data, and many of the largest companies in the world—Facebook, Google, and the like—are supported by revenue generated from the collection of this data for the use of targeted ads.

While these companies clearly have dominance in this space, many of the benefits of this data collection trickle down to small businesses and create a more tailored online experience for consumers.

For example, a local greenhouse can use their limited time and resources to advertise in the most effective way for less cost by using targeted ads. Instead of publishing an imprecise catch-all ad in the newspaper, they can purchase ad space on websites dedicated to gardening or set up a geolocation range for IP addresses in driving distance in their greenhouse.

This ensures that their ad is reaching their most likely group of customers—avid gardeners who live within 10 miles of the greenhouse. In the same transaction, the gardeners benefit from knowing what promotions and deals are available in their home area.

To some consumers, these practices can feel like an invasion of privacy, or leave them wondering how much personal information about them is being sold. As this subcommittee continues to grapple with the many privacy issues and data breaches of the past few years, we are no stranger to the risks of collecting such detailed consumer profiles and amassing it in centralized data repositories susceptible to bad actors.

This hearing is yet another opportunity to discuss these risks and understand what those are in the private sector—and what those are in the private sector are doing to address them.

Additionally, ads are only effective if they're reaching actual people. Digital ad fraud and the scourge of traffic bots, algorithms designed to look like actual humans, complicate this system in new ways, and undermine the trust in the current advertising model.

Businesses who think they are paying for ad space because of high audience interest might not get the response they want because of bots. One study found that 22 percent of desktop video ads were viewed only by bots.

The online advertising ecosystem has many players that contribute to its effectiveness. Understanding how each of these play-

ers interact with each other and with consumers is an important step in discussing larger issues like privacy and data security.

As always, it is one of the primary goals of the Energy and Commerce Committee to ensure that consumers are informed and can make educated decisions about their online habits.

The advertising-based model supports the platforms that we use to communicate, connect, shop, and work. Today, we hope to hear of the many efforts undertaken by industry to innovate and grow in this space, while at the same time responding to consumer demands for privacy and security of their data.

[The prepared statement of Mr. Latta follows:]

PREPARED STATEMENT OF HON. ROBERT E. LATTA

Good morning and thank you to all our witnesses for joining us today. An advertisement used to mean a quarter page section in your local newspaper, a billboard along the highway, or as our chairman of the full committee would know, a radio spot during the rush-hour commute. While those types of advertisements still exist, targeted digital advertising has begun to dominate the advertising and marketing industry.

The digital advertising ecosystem is complex and often misunderstood. Today, we hope to clear up some of that confusion for consumers and discuss both the benefits and emerging, often high profile, challenges of online advertising. Our expert panel of witnesses will explain how this technology works, and its place in our economy and our lives.

According to the Interactive Advertising Bureau, the ad-supported internet ecosystem generated over $1 trillion for the U.S. economy in 2016 and was responsible for 10.4 million jobs with 44 percent of those jobs employed by small and medium businesses. The massive growth of online advertising's contribution to GDP can be tied to improved data collection and subsequent ad targeting.

Digital ads are dependent on consumer-related information and data, and many of the largest companies in the world, Facebook, Google, and the like, are supported by revenue generated from the collection of this data for the use of targeted ads. While these companies clearly have dominance in this space, many of the benefits of this data collection trickle down to small businesses and create a more tailored online experience for consumers.

For example, a local greenhouse can use their limited time and resources to advertise in the most effective way for less cost by using targeted ads. Instead of publishing an imprecise, catch-all ad in the newspaper, they can purchase ad space on websites dedicated to gardening or set up a geolocation range for IP addresses in driving distance to their greenhouse. This ensures that their ad is reaching their most-likely group of customers: avid gardeners who live within 10 miles of the greenhouse. In the same transaction, the gardeners benefit from knowing what promotions and deals are available in their area.

To some consumers, these practices can feel like an invasion of privacy, or leave them wondering how much personal information about them is being sold. As this subcommittee continues to grapple with the many privacy issues and data breaches of the past few years, we are no stranger to the risks of collecting such detailed consumer profiles and amassing it in centralized data repositories susceptible to bad actors. This hearing is yet another opportunity to discuss these risks and understand what those in the private sector are doing to address them.

Additionally, ads are only effective if they're reaching actual people. Digital ad fraud and the scourge of traffic bots, algorithms designed to look like actual human views, complicate this system in new ways, and undermine the trust in the current advertising model. Businesses who think they are paying more for ad space because of high audience interest, might not get the response they want because of bots. One study found that 22 percent of desktop video ads were viewed only by bots.

The online advertising ecosystem has many players that contribute to its effectiveness. Understanding how each of these players interact with each other and with consumers is an important step in discussing larger issues like privacy and data security. As always, it is one of the primary goals of the Energy and Commerce Committee to ensure that consumers are informed and can make educated decisions about their online habits.

The advertising-based model supports the platforms that we use to communicate, connect, shop, and work. Today, we hope to hear of the many efforts undertaken

by industry to innovate and grow in this space, while at the same time responding to consumer demands for privacy and security of their data.

Thank you to all of our witnesses for being here today. I yield to the gentle lady from Illinois, the ranking member of the subcommittee, for a 5-minute opening statement.

Mr. LATTA. Again, I want to thank our witnesses for being with us today, and at this time I will yield back my time and recognize the gentlelady from Illinois, the ranking member of the subcommittee, for 5 minutes.

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

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

Ads are ubiquitous, often irritating, as you browse the internet. Most of the time, we give little thought to why those ads are there.

But, as we touched on during the Facebook hearing earlier this year, the ads that consumers see are often highly targeted.

I've certainly noticed them in my own experience that I am being tracked online. I start to shop on a website and then next thing you know an ad for the very same product I was looking for turns up on a completely different website.

Companies may claim that consumers like targeted ads, and some may. But consumers tell a different story often when they are polled. In fact, most Americans report taking at least some steps to block tracking.

Americans are realizing how little control they have over their own information. You may not even be on Facebook, but Facebook collects information about you.

You can block cookies but you are still tracked. You are tracked regardless of whether you're on a computer, smartphone, or tablet, and the internet of things expands which devices can collect your data even further.

The use of targeted digital ads can have serious consequences. It's not just online shopping. We have learned more and more in the past year about how Russia used targeted ads to spread disinformation and meddle in our elections.

The grand jury in Special Counsel Robert Mueller's investigation has indicted 13 Russian nationals and three companies for waging information warfare on the United States.

Targeted ads can also be tools for discrimination. A ProPublica investigation last year found that Amazon, Verizon, UPS, and Facebook all posted jobs—job ads that were targeted specifically to specific age groups, excluding older Americans.

We have also seen ads for junk financial products that are directed to communities of color. Facebook has now removed the option to exclude certain ethnic groups for advertising. But the potential for discrimination remains in the online ad market.

Congress has been woefully slow in responding to the risks that online advertising practices pose to privacy, fairness, and our very democracy.

The Federal Trade Commission does not have the resources it needs to be an effective consumer watch dog. It does not have close

to enough staff to monitor anti-consumer practices online and it has weak enforcement tools.

The FTC has limited rulemaking authority. It cannot impose civil penalties right away. When a company fails to protect consumer privacy, instead it has to negotiate a consent order and only if it later finds a violation of that consent order does a company actually pay for misusing consumer data.

Perversely, the Republican majority tried the last Congress to further restrict the FTC's authority. Fortunately, that legislation was not passed.

Consumers deserve a real protection. We need rules of the road for what information can be collected and stored on—and stored about consumers.

Consumers need real options when it comes to how their information is used. The Facebook scandal and the many data breaches in recent years have made consumers increasingly aware of how much data is sitting out there—how much of their own data.

After the Equifax data breach, we had a witness describe the steps a consumer could take to protect the information, and she basically made protecting your privacy sound like a full time job.

It shouldn't be that way. I am glad that we are having this—we are continuing to discuss the field of digital ads. My question is what comes next.

Is the subcommittee finally going to take up legislation to strengthen consumer privacy protection? This is a complicated issue.

But I believe that we are up to the challenge. Let's bring our ideas to the table and hash out the solutions that are—that our constituents deserve.

People are fed up with big corporations tracking their every move online and controlling what they see. They are demanding action and it is time for Congress, for this committee, to deliver.

I yield back.

Mr. LATTA. Thank you very much. The gentlelady yields back, and I believe the chairman of the full committee has not arrived yet. Is there anyone on the Republican side wishing to claim the chairman's time?

If not, at this time I will recognize the gentleman from New Jersey, the ranking member of the full committee, for 5 minutes.

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

Mr. PALLONE. Thank you, Mr. Chairman.

Today's hearing will explore online advertising and its role in society. In the early days of the internet, online advertising was like other forms of advertising.

Advertisers would place ads aimed at broad audiences. But that has all changed. Advertising is now directed to smaller targeted categories of audiences, those most likely to purchase their products and services.

Targeted advertising can provide more relevant advertising to consumers. It also provides revenue to advertisers.

For example it allows a small business selling boutique men's razors to reach men, say, in their 40s and 50s who may be able to afford a specialty product.

However, it also allows a scammer to reach women over a 65 in a particular zip code who have been duped in the past to give their money to fake veterans charities.

Moreover, contrary to industry claims, it's not always anonymous. Right now, anyone willing to pay can target advertising to a list of 20 names and send a specialized adjust to them.

Without explaining or justifying the list, an advertiser could send an advertisement to 20 specific people who have a mental health condition or are taking a particular medication.

And target advertising is possible because of the vast amounts of information collected about individual consumers by companies across the advertising ecosystem.

Beyond the websites, you go to the advertisers today to see there are numerous middlemen, ad networks, ad agencies, data brokers, and the like.

These companies lurk in the background, often unknown to consumers, and not just collecting and storing data that would choose to share. They track what websites we visit, what purchases we make, and even the movement of your mouse on the computer screen.

And information collected about our online activity is increasingly being merged with our offline identity to create extremely detailed profiled.

Moreover, they can go beyond facts to include inferences about our interests and demographic information. Targeted advertising by its very nature separates people into categories and shapes our choices.

We have shown limited options that are chosen for us by automated processes based on our profiles. So what I see on the internet may end up being very different from what you see, and neither of us getting all the information that may help us make our purchasing decisions.

Even if we seek out additional information we may get created content, further limiting our choices.

In addition to the risks of scams, targeted ads can result in blatant discrimination. It's been well documented than targeted advertising systems have allowed housing ads to exclude people of color and job ads to exclude older workers.

At this committee's hearing last year on the effect of algorithms on consumers we discussed how bias can be built into algorithms, resulting in bias results, and that problem does not just apply to content and search results. It applies to advertisement as well.

It is good that Google and Bing have now blocked ads for predatory payday loans, but that's not enough. The American people rightfully feel like they've lost control.

One survey showed that 84 percent of people want more control over what companies can learn about them online, yet 65 percent of people are resigned to the fact that they have little control.

So we hear a lot about self-regulatory transparency, notice, and choice but we all receive many updated privacy policies spurred by the EU's new data privacy regulations. None of us have time to

read all of them, let alone actually understand and remember what each company is doing with our data.

And what about the companies collecting our data that we don't even know exist?

The Equifax breach brought that issue up front and center, and people weren't just upset that their data was stolen. They were upset that a company that may have never—they've never interacted with had all that data.

So I think we can do better and I think we must do better, Mr. Chairman. It's time we all admit that the current system just isn't working for consumers, and Congress needs to do a better job and pass comprehensive privacy legislation so people can take back control that they've lost.

And I yield back.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Today's hearing will explore online advertising and its role in society.

In the early days of the internet, online advertising was like other forms of advertising-advertisers would place ads aimed at broad audiences. But that has all changed. Advertising is now directed to smaller, targeted categories of audiences-those most likely to purchase their products and services.

Targeted advertising can provide more relevant advertising to consumers. It also provides revenue to advertisers. For example, it allows a small business selling boutique men's razors to reach men, say in their 40s and 50s, who may be able to afford its specialty product. However, it also allows a scammer to reach women over 85, in a particular zip code, who have been duped in the past to give their money to fake veterans' charities.

Moreover, contrary to industry claims, it is not always anonymous. Right now, anyone willing to pay, can target advertising to a list of 20 names and send a specialized ad just to them. Without explaining or justifying the list, an advertiser could send an advertisement to 20 specific people who have a mental health condition or are taking a particular medicine.

Targeted advertising is possible because of the vast amounts of information collected about individual consumers by companies across the advertising ecosystem. Beyond the websites you go to and the advertisers whose ads you see, there are numerous middlemen-ad networks, ad agencies, data brokers, and others.

These companies lurk in the background, often unknown to consumers. They are not just collecting and storing data that we choose to share. They track what websites we visit, what purchases we make, and even the movement of your mouse on the computer screen. And information collected about our online activity is increasingly being merged with our offline identity to create extremely detailed profiles. Also, they can go beyond facts to include inferences about our interests and demographic information.

Targeted advertising, by its very nature, separates people into categories and shapes our choices. We are shown limited options that are chosen for us by automated processes based on our profiles.

So, what I see on the internet may end up being very different from what you see. And neither of us is getting all the information that may help us make our purchasing decisions. Even if we seek out additional information, we get curated content further limiting our choices.

In addition to the risk of scams, targeted ads can result in blatant discrimination. It's been well-documented that targeted advertising systems have allowed housing ads to exclude people of color and job ads to exclude older workers.

At this committee's hearing last year on the effect of algorithms on consumers, we discussed how bias can be built into algorithms resulting in biased results. That problem does not just apply to content and search results, it applies to advertisements as well. It is good that Google and Bing have now blocked ads for predatory payday loans, but it is not enough.

The American people rightfully feel like they've lost control. One survey showed that 84 percent of people want more control over what companies can learn about them online yet 65 percent of people are resigned to the fact they have little control.

We hear a lot about self-regulatory transparency, notice, and choice, but we all received many updated privacy policies spurred by the EU's new data privacy regulations. None of us have time to read all of them, let alone actually understand and remember what each company is doing with our data.

And what about the companies collecting our data that we don't even know exist. The Equifax breach brought that issue front and center. People weren't just upset that their data was stolen. They were upset that a company that they may have never interacted with had all that data.

We can do better, and we must do better. It's time we all admit that the current system just isn't working for consumers. Congress needs to do its job and pass comprehensive privacy legislation so people can take back control.

Thank you, I yield back.

Mr. LATTA. Thank you very much. The gentleman yields back the balance of his time.

And that now concludes Member opening statements. The Chair reminds Members that, pursuant to committee rules, all Members' opening statements will be made part of the record.

Again, I want to thank our witnesses for being with us today and taking time to testify.

Today's witnesses will have the opportunity to give a 5-minute opening statement followed by a round of questions from the Members.

Our witness panel for today's hearing will include Ms. Rachel Glasser, who is the global chief privacy officer at Wunderman; Mr. Mike Zaneis, president and CEO of Trustworthy Accountability Group; Mr. Justin Brookman, the director of privacy and technology policy at Consumers Union; and Dr. Howard Beales, professor of strategic management and public policy at George Washington University.

Again, we want to thank you all for being with us and taking the time to testify and, again, Ms. Glasser, you're recognized for 5 minutes for your opening statement. So just pull that mic up close and press the button to get her on, and we appreciate hearing your testimony today.

Thanks very much.

STATEMENTS OF RACHEL GLASSER, CHIEF PRIVACY OFFICER, WUNDERMAN; MIKE ZANEIS, PRESIDENT AND CHIEF EXECUTIVE OFFICER, TRUSTWORTHY ACCOUNTABILITY GROUP; JUSTIN BROOKMAN, DIRECTOR, PRIVACY AND TECHNOLOGY POLICY, CONSUMERS UNION; J. HOWARD BEALES III, PH.D., PROFESSOR OF STRATEGIC MANAGEMENT AND PUBLIC POLICY, GEORGE WASHINGTON SCHOOL OF BUSINESS

STATEMENT OF RACHEL GLASSER

Ms. GLASSER. Thank you very much, Chairman Latta, Ranking Member Schakowsky, and members of the subcommittee.

Good morning, and thank you for the opportunity to speak at this important hearing. I am honored to have traveled from New York to appear before you to today to discuss how responsible digital advertising supports innovative, diverse, and free services that are the foundation of our online economy.

My name is Rachel Glasser. I am the global chief privacy officer for Wunderman, who's the parent company of KBMG.

I am responsible for data privacy strategy and implementation and ongoing process improvements for all of Wunderman including KBMG.

KBMG is headquartered in Louisville, Colorado, with offices in New York, Texas, and Brazil. We help brands, companies, and nonprofit, large and small, use data as a strategic asset and provide data-driven marketing engagement for improved marketing performance and a resident customer experience.

The internet has drastically improved the way people work, consume content, learn, travel, access health care, spend leisure time, and communicate with one another.

Many of these life changing benefits are available to consumers for free because it's supported by digital advertising. In short, digital advertising is the lifeblood of the internet economy and connects business with consumers who are most likely to value their products and services.

Data is at the center of this American success story and is core to the marketing services that KBMG provides the clients.

Accordingly, the foundation of our business model is trust. We work every day to earn and maintain the trust of both consumers and companies with whom we work.

My job is to help ensure that privacy and respect for the consumer are integrated into every initiative.

This message comes from the top. Respect consumer privacy, be transparent about our data collection and use practices, offer consumer choice, and honor those choices.

This trust allows us to innovate faster, provide more value to clients, and create better experiences for consumers.

Digital advertising is a broad term used to describe the paid advertising that publishers put on their websites or apps. It enables these publishers to provide consumers with content and services for free.

Today, I am focusing on digital advertising tailored to consumers' likely interests. This is generally known as interest-based advertising, or IBA.

IBA is why consumers see ads that are relevant to their interests. With this type of advertising, companies and advertisers collect information across some of the sites and apps that they visit.

This information is then used to predict what ads might be the most interesting to consumers. IBA doesn't depend on information that may be personally identifiable such as a consumer's name or a phone number or postal address.

In fact, most ad tech companies do not want to know the identity of a consumer for the purposes of IBA. They only want to link an interest category to demographic data with the consumer's browser so that they can serve up relevant ads.

Of course, different companies may use different methods of IBA. To kind of level set, it's important to go over the fact that there are several different players in the advertising ecosystem.

We have the consumer, the publisher, the advertiser, and the third party advertising company, and that's where my company sits.

We are third party advertising company. As I mentioned, KBMG, as a digital marketing company, places a high priority on consumer privacy and reasonable use of data.

We expect that participants in the online economy will honor high standards regarding the collection and use of online data.

This supplies the publishers, platforms, social media, data management companies, ad tech providers, commerce sites, and more.

At a minimum, when data is collected and used to support various activities such as online advertising or to create personalized experiences, each player in the data life cycle has a responsibility to be transparent, offer consumers appropriate choices, and honor those choices with respect to data collection and use.

We also expect every company to take reasonable measures to secure that data prevent—to secure that data and prevent potential misuse.

This leads me to my final point this morning. Businesses have a vested interest in acting responsibly and building user trust on line. Recognizing the value of user trust and the potential applications of data online, the digital ecosystem has taken initiative and thorough measures to put in place a set of codes and principles to reinforce these practices.

The NAI and the DAA are two self-regulatory groups committed to maintaining and enforcing responsible privacy practices and high standards for data collection.

These standards include providing consumers with enhanced transparency and control and companies like mine voluntarily commit themselves to these organizations.

These companies demonstrate their desire to be good actors and they are obliged to abide by the respective codes and principles. This is a clear indication of the intent of companies to act responsibly, build user trust, and help drive innovation and grow the internet economy.

There is no question that data privacy is on everyone's minds these days. But for our industry it's been on our mind for nearly two decades.

While not to be downplayed by any means, we do not want the recent events of recent to overshadow the extraordinary benefits of the online advertising ecosystem and we are very pleased that the Energy and Commerce Committee is taking the time to learn more about this vibrant and exciting sector.

Thank you.

[The prepared statement of Ms. Glasser follows:]

Testimony of Rachel Glasser, Chief Privacy Officer, Wunderman.

Before the Energy & Commerce Committee,

Subcommittee on Digital Commerce & Consumer Protection

Understanding the Digital Advertising Ecosystem

June 14, 2018

Chairman Latta, Ranking Member Schakowsky, and Members of the Subcommittee, good morning and thank you for the opportunity to speak at this important hearing. I am honored to appear before you today to discuss how responsible digital advertising supports innovative, diverse and free services that are the foundation of our online economy. My name is Rachel Glasser, I am the global Chief Privacy Officer for Wunderman, parent company for KBMG. I am responsible for data privacy strategy and implementation, and on-going process improvements for all of Wunderman including KBMG. I also provide support and mentorship to our employees globally.

KBMG is headquartered in Louisville, Colorado with offices in in New York, Texas, and Brazil with several hundred employees. KBMG is a data analytics and marketing company. We help brands and companies - large and small - and non-profits, use data as a strategic asset and provide data-driven marketing engagement for improved marketing performance and more resonant consumer experiences. We combine data, sophisticated analytics, actionable insights, and marketing technology to optimize engagement across different platforms including email, mobile, social, display, and others, throughout the customer lifecycle.

The Internet has drastically improved the way people work, consume goods and media, learn, travel, access health care, spend leisure time, and communicate with one another. Many of these life-changing benefits are available to consumers for free, supported by digital advertising. In short, digital advertising is the lifeblood for the Internet economy and connects American businesses large and small with consumers most likely to value their products and services.

Data is at the center of this American success story. I see the benefits of this every day at my office in NY. All companies today – from the giants of Wall Street to the corner store on Main Street – rely upon the responsible use of data to improve consumer experiences and develop relevant marketing. Relevant advertising links people with the right products and services and perhaps most importantly supports a previously unimaginable array of free products and services.

Data is core to the marketing services that KBMG provides to our clients. The foundation of our business model is trust. As long-established data experts, KBMG has built a business and reputation on the understanding that the ability to use and process consumer data can only occur in an environment where we earn the trust of both consumers and the companies with whom we work. With the full support of our senior leadership, my job is to help ensure that privacy and respect for the consumer are integrated into every initiative. This message comes from the top: respect consumer privacy, be transparent about our data collection and use practices, offer consumers choice and honor those choices. This trust allows us to innovate faster, provide more value to our clients, and create better experiences for consumers. It is this constant drive to innovate that drives the US economy.[1]

In my testimony, I will briefly address: (1) how Interest-Based Advertising provides value to consumers, advertisers, publishers and our economy; (2) the role and responsibilities of different stakeholders in the digital advertising ecosystem; (3) the types of information used in digital advertising; and (4) the proactive steps industry has taken to protect consumers through effective self-regulation.

1) <u>Digital Advertising: A Brief Overview</u>

Digital Advertising is a broad term used to describe the paid advertising that publishers put on their websites or apps to enable them to provide consumers with content and services for free. Some digital advertising is tailored to consumers' likely interests by companies promoting

[1] https://www.mckinsey.com/~/media/McKinsey/Industries/High%20Tech/Our%20Insights/The%20great%20transformer/MGI_Impact_of_Internet_on_economic_growth.ashx

their products or services. This is generally known as Interest-Based Advertising (IBA), when it occurs across websites, and Cross-App Advertising (CAA), when it occurs across applications (apps).

IBA/CAA is why consumers see ads that are relevant to their specific interests. With this type of advertising, companies and advertisers collect information across some of the sites consumers visit and apps that they use. This information is then used to try to predict what ads might be the most interesting to individual consumers. IBA/CAA doesn't depend on information that may be personally identifiable, such as a consumer's name, phone number, Social Security number, etc. In fact, most ad tech companies don't want to know the identity of a consumer for IBA/CAA. They only want to link interest categories (loves travel) or demographic data (male under 30) with a consumer's browser so that they can serve up relevant ads. Of course, different companies use different methods of IBA/CAA.

The basic way consumers are placed into an interest category or group on a browser is based on a consumer's visits to websites. Let's say an ad-tech company partnered with a clothing retail website that a consumer visits. That ad tech company would assign an ID to the consumer's browser usually by storing a unique ID number in a text file or cookie on the browser. This is then matched to a "clothing shopper" category by pairing that ID number with interest categories/groups in an online database.

Unique ID Number	**Matched Categories**
450982374	"Male", "Age 25-34","clothing"

Other information can be used to match a consumer into a group, as well. For example, if the consumer has previously purchased oxford shirts from that retail website, the website could tell the company to also match "oxford shirt buyer" to the ID.

There are several different players in the online ad ecosystem:

- *The consumer*
- *Publisher:* The individual or business in charge of a website or app. They sell advertising space on their websites and apps to advertisers.
- *Advertiser:* The individual or business that has a product or service they want to advertise. They buy advertising space on websites and apps.
- *Third-Party Advertising Company:* Websites and apps usually do not play a direct role in choosing the ads consumers see. Instead, a third-party advertising technology company manages the target audience, ad selection, and placement for both the publisher and advertiser. It makes the process more efficient for everyone.

As a general rule, IBA/CAA does not depend on information that personally identifies a consumer such as name, e-mail address, phone number, photographs, etc. Rather than using personally identifiable information, most IBA/CAA that uses randomly-generated numbers to match a specific web browser or mobile device with interest categories.[2]

2) <u>The Responsible Use of Data Is Everyone's Responsibility</u>

Recent events have raised questions about the use of data for digital advertising. In some cases, the diverse range of business practices and advertising models have caused confusion. This concerns me because most actors engage in the responsible, ethical and transparent use of information.

As I already mentioned, KBMG as a digital marketing company places a high priority on consumer privacy and the responsible use of data. Given how information is collected and shared in today's digital ecosystem, we expect that every participant in the online economy will honor high standards regarding the collection and use of online data. This applies to publishers,

[2] http://www.networkadvertising.org/understanding-online-advertising/how-does-it-work/

platforms, social media, data management companies, ad tech providers, analytics firms, and ecommerce sites. At a minimum, when data is collected and used to support various activities such as online advertising or to create personalized online experiences, each player in the data life cycle and advertising ecosystem has a responsibility to be transparent about the use of that data, offer consumers appropriate choices about the collection and use of data, and honor those choices. We also expect every company to take reasonable measures to secure that data and prevent potential misuse.

There is near-universal agreement across our ecosystem that transparency is critical, particularly as we continue to innovate and develop more effective, efficient and exciting ways to engage with consumers. The purpose is clear: provide consumers with information that explains in plain English what data is being collected and for what purpose as they navigate across a website or engage with a mobile application. We cannot build trust without being transparent about our practices. And without trust we cannot expect consumers to be willing to share their data. Without data, we cannot provide consumers with the wide range of online products, services, and rich content that is available online today, often at no cost to the consumer.

Transparency through website privacy notices or enhanced privacy notices[3] has been the customary means by which this information is communicated. Industry, however, is constantly innovating and seeking news ways to provide consumers with the most important information at just the right time. Indeed, self-regulatory bodies such as the Digital Advertising Alliance[4] (DAA) and the Network Advertising Initiative[5] (NAI) require participants and members to provide transparency through the use of an icon on advertisements and a centralized industry

[3] https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf "Implementation of Transparency and Consumer Control Principles", page 9.
[4] https://www.digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf Principles II Transparency; page 33 of the commentary.
[5] http://www.networkadvertising.org/sites/default/files/nai_code2018.pdf II.B Transparency and Notice; page 19 of the commentary.

website in addition to privacy policies. Efforts to innovate in this area continue as technologies evolve.

Transparency is only one component of responsible data use. Companies like KBMG not only describe the purpose for which the data is collected, we take steps to ensure that the data is used in the manner that was described. We also offer consumers appropriate choice and take steps to ensure that choice is respected. Here too each actor in the industry has a responsibility to ensure data is being used for the right purpose and consumer choice is honored. As the CPO of KBMG, I expect that from our business partners, and I work hard to ensure that our partners engage in responsible practices through contract terms, oversight, audits, general due diligence and other mechanisms. Like other companies, we want users to be able to express preferences and be able to make informed decisions about their data and how it is used.

KBMG and all responsible actors in the digital advertising ecosystem honor the principles of transparency and consumer choice because it fosters trust and is the right thing to do. Further, when data is misused it has a downstream negative impact on the entire industry. Consumers become less likely to trust marketers and brands, online platforms, and publishers. And when they are less likely to share their data it becomes more difficult to continue to provide free access to services, personalized content, and drive innovation.

Of course, in some contexts – those can that can cause real consumer harm - the misuse of consumer information may be unlawful. Compliance with myriad state and federal laws is a powerful motivator and we support prohibitions on practices that can cause serious harm to consumers. Even when serious harm may not be an issue, companies should honor their promises to consumers.

3) **Sensitivity, Context, and the Potential for Harm**

The US approach to consumer privacy correctly recognizes that not all information is equally sensitive or presents a risk of harm. The level of transparency and choice needed in a given context should correlate to the level of sensitivity of the data. The more personal, or sensitive the data, the more transparency and choice are critical. Recent events have highlighted instances where personally identifiable information was in fact used and shared. But using and sharing a consumer's name or similarly identifiable information is not necessary in many cases to provide rich, personalized, and relevant advertising. Similarly, inferring a consumer's general location such as a city or county creates less concern than collecting a person's precise location over time. Moreover, we know that different uses of data generate different levels of concern for consumers. Information used to determine eligibility for a benefit or loan presents a greater potential risk of harm to consumers than serving as online ad based on a user's perceived interests. Similarly, uses of data that produce clear value to consumers are more likely to be embraced by consumers than other, unanticipated uses that offer no direct benefit or – in extreme cases – cause material and significant harm.

Industry invests tremendous efforts to provide transparency, notice and choice when it would be most valuable to consumers. For example, stakeholders agree that broad transparency would generally suffice where data is collected for site analytics and aggregated. This use is critical for website operators to better understand how users interact with their site generally, what content and features are popular, and how to make a service or website more user friendly. In this instance, a choice mechanism is not always required or called for and a broad disclosure about site analytics would suffice. This data helps companies improve the basic online user experience and drives businesses to build and improve on features and tools to further that end. As the FTC has noted, not only is choice not necessary in every circumstance, offering choice in such cases is counterproductive.

On the other hand, when data is collected and used for Interest-Based Advertising, where devices can be linked and the data is arguably more granular, industry provides more

transparency and offer consumers the ability to exercise choice.[6] This increased transparency includes ideas like enhanced notice, more specific disclosures within a privacy notice, including specific data points included, and the fact that it data be used for IBA. This increased level of transparency is meant to help users have a better understanding of the intended use of the data and to help them make an informed decision of how they want the data to be used. This too helps build user trust and the flow of data.

4) **Industry Self-Regulation Works**

Businesses have a vested interest in acting responsibly and building user trust online. Recognizing the value of user trust and the potential applications for data online, the digital ecosystem has taken initiative and thorough measures to put in place a set of codes and principles to reinforce responsible practices. The DAA and the NAI are two self-regulatory groups committed to promoting the health of the online ecosystem by maintaining and enforcing responsible privacy practices and high standards for data collection and use for advertising online. These standards include providing consumers with enhanced transparency and control.[7],[8]

Companies voluntarily commit themselves to these organizations. These companies are demonstrating their desire to be good actors and are obliged to abide by the respective codes and principles. This is a clear indication of the intent of companies to act responsibly, build user trust and help drive innovation and grow the Internet economy.

Self-regulation is not just about making promises. Both NAI and DAA are backed up by robust compliance and enforcement mechanisms. NAI, for example, reviews every member company's compliance on an ongoing basis and publishes a compliance report each year. Enforcement of the DAA principles is carried out by the Accountability Program at the BBB.

---

[6] https://www.digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf
[7] http://www.aboutads.info/
[8] http://www.networkadvertising.org/about-nai/

Industry recognizes that the bad or irresponsible practices of a handful of actors will undermine the entire ecosystem. That's why industry has invested tens of millions of dollars in self-regulatory efforts that evolve as our industry evolves.

Conclusion

There is no question that data privacy is on everyone's mind these days. But for our industry, it has been on our minds for nearly two decades. Data is critical to the growth and innovation of the Internet. It adds value to our experiences online and allows brands and marketers to better connect with their consumers. It fosters education, growth, and communication. Trust is essential for continued growth and innovation on the ad supported free internet. Without trust we cannot expect to continue the value exchange and provide free access of information and other free tools and resources to the public, and the growth of our Internet economy. We do not want recent events to overshadow the extraordinary benefits of the online advertising ecosystem and we are pleased that the Energy and Commerce Committee is taking the time to learn more about this vibrant, exciting sector.

Mr. LATTA. Well, thank you for your testimony this morning, and Mr. Zaneis, you are recognized for 5 minutes.

STATEMENT OF MIKE ZANEIS

Mr. ZANEIS. Thank you, Chairman Latta, Ranking Member Schakowsky, distinguished members of the subcommittee, it's wonderful to be before you again today.

May name is Mike Zaneis. I am the president and CEO of the Trustworthy Accountability Group, or TAG, as it's known in the industry.

TAG is a industry not-for-profit organization whose mission is to fight criminal activity throughout the digital advertising supply chain.

It may come as a surprise to all of you that that's a necessary mission. But let me assure you it is. Our industry is fighting the same criminal networks that operate globally often to commit human trafficking, drug trafficking, and widespread digital identity theft.

Why is that? It's because digital advertising is the engine that drives America Mr. Justin BrookmanDirector, Privacy and Technology Policy, Consumers Union's digital data-driven economy.

This is an industry that contributed $1.12 trillion to the domestic economy in 2016 and in so doing created 10.4 million jobs, and these are incredibly high quality jobs that pay very well, spread across the country in literally every congressional district.

With that prosperity, though, comes added attention, as I mentioned. The complexity then Ms. Glasser talked about with the digital supply chain—the fact that you may have dozens of companies touching an ad from the marketer, the agency, the tech firms, all the way down to the publisher before it ever appears, hopefully, in front of a real consumer, creates sometimes an opaque supply chain and that allows criminals to hide in the dark murky corners and to infiltrate it.

It's estimated then that this criminal activity, as I mentioned, causes more than $8.2 billion in harm. But that's just domestically, and the impact is greater globally.

The industry found a common chain of criminal activity a few years ago. The first link in this chain is the theft of digital content. Criminals don't take the time or the effort to create content like our own homegrown creative community does.

Instead, they steal it. Maybe it's a blog posting, a local news article, all the way up to the latest music and movies, and they put this content on websites that they own, and that's because domains are inexpensive and easily accessible.

Once they have a website with quality content on it, they have to generate an audience to visit that website. That's very difficult to do.

Here, again, criminals, of course, cheat, as they always do. They prefer to distribute malware onto consumers' computers and devices.

Once infected, that device can actually open up individual browsers or even behind-the-scenes mobile apps, unbeknownst to the consumer, and it visits Web sites.

We call this fraudulent nonhuman traffic. That's because there's not a person on the other end of that screen. It's estimated then to digital app at a cost to the industry $4 billion a year here in the U.S.

Finally, now that a criminal network has a website with great content, they have what appears to be large engaged audience. They're a perfect candidate to attract digital advertising revenue.

Like any legitimate business, they can embed ads into that site and begin to receive revenue into a matter of weeks a great democratization tool for small businesses in this country.

TAG was created by the industry to solve these challenges. And so we are often referred to as sort of the good housekeeping seal of approval.

To date, the industry has rallied behind these efforts, although we are only 3 years old. More than 680 companies have applied to join TAG.

That's spread across 27 countries and six continents. Most importantly, more than 100 companies have already achieved a TAG certification.

What that means is that these companies are living up to the highest standards using the best technology to fight fraud, to fight ad-supported piracy, to fight malware, and also we have an overarching goal of increasing transparency throughout the supply chain.

We've been very gratified to learn over the past year that these programs are working. Two pieces of independent research showed that in our anti-fraud program that if marketers worked with TAG-certified entities through what we call a TAG-certified channel, they could remove at least 83 percent of those fraudulent nonhuman impressions that they receive. It can save them billions of dollars a year.

With our anti-piracy efforts, a study by EY—Ernst and Young—found that industry efforts to keep ads off of sites and steal content and have illicit material on them had kept more than half of that revenue from flowing to these pirate sites.

I think most encouraging about that research is that the little revenue that does flow to pirate sites comes from nonpremium marketers, meaning the smaller, less reputable folks.

So I appreciate the opportunity to speak to you today and I look forward to answering your questions.

[The prepared statement of Mr. Zaneis follows:]

Written Testimony of Mike Zaneis
President and CEO, Trustworthy Accountability Group

U.S. House of Representatives, Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection

Hearing Entitled "Understanding the Digital Advertising Ecosystem"

June 14, 2018

Chairman Latta, Ranking Member Schakowsky, and distinguished Members of the Subcommittee, it is an honor to appear before you today at this important hearing to better understand the digital advertising ecosystem. In the past, I have been fortunate to testify twice before this Subcommittee on issues impacting our industry; as well as briefing the Subcommittee's Privacy Working Group several years ago. These are vital issues impacting the core of America's digital and data-driven economy.

Today, I come before you wearing a slightly different hat. As the President and CEO of the Trustworthy Accountability Group, or "TAG", I run an industry organization focused on fighting criminal activity in the digital advertising supply chain. In 2016, research showed that such criminal activity – primarily in the form of malware distribution, ad-supported piracy, and advertising fraud – had cost the U.S. economy at least $8.2 billion.[1] However, since that time, the digital advertising industry has joined hands and fought back hard, developing and supporting strong self-regulatory standards that have proven effective in significantly decreasing this negative economic impact.

---

[1] Ernst & Young LLP. (November 2015). What is an Untrustworthy Supply Chain Costing the US Digital Advertising Industry: IAB US Benchmarking Study. Retrieved from https://www.iab.com/wpcontent/uploads/2015/11/IAB_EY_Report.pdf.

I. Digital Advertising is the Engine that Powers the Internet Economy

Digital advertising is the predominant means of supporting both large and small digital businesses. This has always been the case, as a dispersed advertising supply chain democratized the digital economy by allowing anyone with a website to imbed ads and begin receiving revenue within a matter of weeks. This trend continues as consumers and time spent with media shifts towards mobile devices and high-quality video content.

A recent study by the Interactive Advertising Bureau ("IAB") found that the ad-supported internet ecosystem generated $1.12 trillion for the U.S. economy and was responsible for 10.4 million U.S. jobs in 2016, accounting for 7.3 percent of the country's total non-farm employment. The industry doubled both the number of digital advertising jobs and its economic contribution from 2012 to 2016, and increased its employment by 19.6 percent annually during that same period, while the U.S. total non-farm employment grew by just 1.8 percent in that period.

The ad-supported internet ecosystem accounts for 6 percent of the U.S. gross domestic product ("GDP"), representing a 20 percent compound annual growth rate from 2012 to 2016 – five times the average American GDP growth during the same period. These important economic and employment impacts are not restricted to conventional centers of internet industry concentration. Instead, 86 percent of the ad-supported internet economy's direct employment and value currently lie outside the San Francisco Bay Area, New York's Manhattan, Virginia's Arlington County, Boston's Route 128, and the Seattle/Tacoma area. Today, every U.S. Congressional district boasts jobs created by the ad-supported internet, with some of the biggest numbers of jobs in such states as North Carolina, Texas, and Utah.[2]

[2] Prof. John Deighton, the Baker Foundation Professor and the Harold M. Brierley Professor of Business Administration, Emeritus, at the Harvard Business School. (March 2017). The Economic Value of the Advertising-

II. With Prosperity Comes Threats and Challenges

The tremendous economic and employment growth seen in the digital advertising industry has made it one of the most important industries in the U.S. – and one of the most targeted by criminal enterprises. Fraudulent impressions, infringed content, and malvertising cost the U.S. digital marketing, advertising, and media industry $8.2 billion annually. More than half of these losses derive from "non-human traffic" – fake advertising impressions that are neither generated by real consumers nor received by actual marketers. Eliminating these fraudulent impressions would save advertisers more than $4 billion annually.[3] The aforementioned IAB study identified three primary supply chain costs:

- Invalid Traffic – As described above, ad fraud accounts for the largest portion of costs, at a total of $4.6 billion. Seventy-two percent of the loss associated with the web's fraudulent traffic happens on desktops and 28 percent on mobile.
- Infringed Content – At $2.4 billion, infringed content – stolen video programming, music, and other editorial content that is illegally distributed on the web – represents the most significant share of lost revenue opportunity costs. Two billion dollars of that total is based on an estimate of approximately 21 million U.S. consumers' willingness to spend $8 per month on what is currently classified as infringed content. The additional $456 million represents the loss of potential advertising dollars. The findings show that unless the industry takes significant steps, there is a likelihood that the number of people consuming stolen content on digital platforms will increase.

Supported Internet Ecosystem. Retrieved from https://www.iab.com/news/ad-supported-internet-brings-1-trillion-u-s-economy-doubling-contribution-since-2012-according-iab-study/.

[3] Ernst & Young LLP. (November 2015). What is an Untrustworthy Supply Chain Costing the US Digital Advertising Industry: IAB US Benchmarking Study. Retrieved from https://www.iab.com/wpcontent/uploads/2015/11/IAB_EY_Report.pdf.

- Malvertising-Related Activities – Combating malware that can be distributed within digital advertising creative, often referred to as "Malvertising", comes in at $1.1 billion, with $781 million of those losses being generated from ad blocking instigated due to security and malware concerns. Costs associated with investigating, remediating, and documenting direct incidents of malicious advertising total $204 million. The consumer costs inflicted by malvertising are likely to be even higher than industry costs.

Each of these seemingly unrelated crimes actually represent a single link in an interconnected chain of criminal activity. Rather than investing millions of dollars in creating quality, original content, criminal networks prefer to steal digital content. Once misappropriated, this content – ranging from simple blog posts or social media photos to platinum grossing music and box office movie hits – can be placed on domains that are cheaply and easily available. Even the best content requires an audience, so criminals then distribute malware that is capable of hijacking consumers' computers and devices. One study shows that internet users are twenty-eight times more likely to get malware from content theft sites.[4] Once under their control, these underground networks can stich thousands of devices together into botnets that are capable of browsing the web or utilizing mobile apps without the consumer being aware of the infection. Armed with this web browsing capacity, criminals can generate what appear to be real human visits to their own websites. Now that the sites have seemingly legitimate content and a large audience, they can attract advertising revenue from legitimate players in the ecosystem, resulting

[4] Digital Citizens Alliance study conducted by RiskIQ. (December 2015). Digital Bait: Internet Users At High Risk Of Malware From Content Theft. Retrieved from https://www.digitalcitizensalliance.org/news/press-releases-2015/digital-bait-internet-users-at-high-risk-of-malware-from-content-theft-70-million-underground-market/.

in advertising fraud. This is the predominant way criminals are able to cause massive harm to consumers and businesses.

III. TAG Represents Effective Industry Self-Regulation to Combat Criminal Activity

Founded in January 2015, TAG is an industry-led 501(c)(6) not-for-profit organization. It is the leading member-based global certification program fighting criminal activity and increasing trust in the digital advertising industry. TAG's mission is to eliminate fraudulent traffic, combat malware, prevent internet piracy, and promote greater transparency in the digital advertising supply chain. TAG advances those initiatives by bringing member companies from across the digital advertising supply chain together in a variety of working groups to set the highest standards for its certification programs in these four areas of our mission. The working groups develop and maintain suites of compliance tools to aid companies in complying with the certification program guidelines. Companies that are shown to abide by the standard for a TAG program can achieve the certification seal for that program and use the seal to publicly communicate their commitment to combatting criminal activity in the digital advertising supply chain.

To date, more than 100 companies have achieved at least one of the certification seals associated with the following four certification programs:

TAG's Certified Against Fraud Program

The mission of the TAG Certified Against Fraud Program is to combat fraudulent, invalid traffic in the digital advertising supply chain. The program provides companies with Certified Against Fraud Guidelines, as well as a suite of anti-fraud tools to aid in compliance:

- The Payment ID System creates a chain of custody for digital advertising transactions, helping companies to ensure that payments made in the digital ad ecosystem are going to legitimate partners.
- The Data Center IP List is a common list of IP addresses with invalid traffic coming from data centers where human traffic is not expected to originate. TAG publishes this list on a monthly basis to assist companies in meeting the requirement in the Certified Against Fraud Guidelines that companies employ data center IP threat filtering across all of the monetizable transactions that they handle.
- The Publisher Sourcing Disclosure Requirements (PSDR) foster trust in the marketplace by disclosing the amount of sourced traffic for a given publisher. This policy tool outlines the requirements for publishers to disclose the volume of traffic acquired through paid sources.
- The Ads.txt Specification creates greater transparency in the inventory supply chain by creating a public record of Authorized Digital Sellers, giving publishers greater control over their inventory in the market, and making it harder for bad actors to profit from selling counterfeit inventory across the ecosystem.

TAG's Certified Against Malware Program

The mission of the TAG Certified Against Malware Program is to eliminate the distribution of malware throughout the digital advertising supply chain. Malware delivered through the advertising ecosystem degrades overall trust in the system by generating a poor consumer experience. Additionally, malware infected machines attack the advertising ecosystem in order to generate money for fraudsters. Because each participant in the ecosystem has

visibility into only their subset of the problem, preventing the delivery of malware overall is challenging, resulting in continued attacks on consumers through the various uncoordinated parts of the system.

The Certified Against Malware Program provides companies with a roadmap by which to combat malware in the digital advertising supply chain effectively, improving consumer experience and stopping botnet attacks that fund fraudsters. By coordinating cross-industry information sharing, TAG enables companies to partner in thwarting attacks that they would not be able to stop alone.

TAG's Certified Against Piracy Program

The mission of the TAG Certified Against Piracy Program is to help advertisers and agencies avoid damage to their brands from ad placement on websites and other media properties that facilitate the distribution of pirated content and counterfeit products. This voluntary initiative helps marketers identify sites that present an unacceptable risk of misappropriating copyrighted content and sell counterfeit goods, and it will help them remove those sites from their advertising distribution chain.

The Certified Against Piracy Program provides companies with the Certified Against Piracy Guidelines, as well as a suite of anti-piracy tools, to aid in compliance with the program requirements.

- In order to achieve the Certified Against Piracy Seal, Direct Buyers must operationalize and comply with the TAG Anti-Piracy Pledge.

- In order to achieve the Certified Against Piracy Seal, Self-Attested DAAPs and Validated DAAPs must meet all of the elements in one or more of the five Core Criteria for Effective Digital Advertising Assurance.

- The TAG Pirate Mobile App List is a common list of mobile apps that were removed from App Stores for infringing on protected intellectual property rights. TAG publishes this list on a quarterly basis to assist companies in meeting the requirement in the Certified Against Piracy Guidelines that companies employ pirate mobile app filtering for all advertising displayed in a mobile app environment.

TAG's Inventory Guidelines Program

The TAG Inventory Quality Guidelines (IQG) Program promotes the flow of advertising budgets into digital advertising with industry regulation that offers a framework for brand safety. The mission of the IQG Program is to reduce friction and foster an environment of trust in the marketplace by providing clear, common language that describes characteristics of advertising inventory and transactions across the advertising value chain. The goals of the IQG Program are to: (i) support the information needs of advertising buyers; (ii) define a common framework of disclosures that sellers can use across the industry; (iii) offer clear language that enables buyers to make informed decisions; and (iv) review compliance and facilitate the resolution of disputes and complaints.

Proven Results

Industry self-regulation is an effective means of addressing the challenges facing the digital advertising ecosystem. During the past year, independent research has measured the effectiveness of TAG's anti-fraud and anti-piracy efforts and found them to be highly successful at combatting criminal activity in the digital advertising supply chain.

In December 2017, The 614 Group released a study commissioned by TAG showing that the use of TAG Certified distribution channels for digital advertising reduced the level of fraud by more than 83% in comparison to broader industry averages. The study was conducted by examining more than 6.5 billion display and video impressions in campaigns run through TAG Certified Channels by three major media agencies for their clients.[5] Among the study's findings:

- Analyses by verification technology providers found the levels of fraud, often referred to as "Invalid Traffic" (IVT), in digital advertising average 8.83 percent for display inventory in North America (and rise to 12.03 percent when video inventory is included).
- The 614 Group examined comparable rates of fraud for campaigns run through "TAG Certified Channels", in which multiple entities involved in the transaction – such as the media agency, buy-side platform, sell-side platform and/or publisher – had achieved the TAG Certified Against Fraud Seal.
- In such TAG Certified Channels, the IVT rate fell to 1.48 percent, a reduction of 83 percent over industry averages.

[5] The 614 Group. (December 2017). TAG Fraud Benchmark Study. Retrieved from https://www.tagtoday.net/fraud_benchmark_research_us.

Similarly, a 2017 Ernst & Young study commission by TAG found that anti-piracy steps taken by the digital advertising industry – including the TAG Certified Against Piracy Program – have reduced ad revenue for pirate sites by between 48 and 61 percent, which represents notable progress against the $2.4 billion problem of infringing content. Among the study's findings:

- Digital ad revenue linked to infringing content was estimated at $111 million last year, the majority of which (83 percent) came from non-premium advertisers.
- If the industry had not taken aggressive steps to reduce piracy, those pirate site operators would have potentially earned an additional $102-$177 million in advertising revenue, depending on the breakdown of premium and non-premium advertisers.
- Ongoing industry efforts against piracy have therefore reduced the advertising revenue of pirate sites by 48 to 61 percent.[6]

This research proves that when the industry works together, it is possible to solve even the most nefarious threats in the digital marketplace.

IV. Collaboration is Prevalent Across the Digital Advertising Ecosystem

A myth promulgated by industry naysayers suggests that, because criminal activity can often provide higher ad revenue to certain parts of the digital supply chain, the industry has a perverse incentive to not police itself. History has shown just the opposite to be true.

[6] Ernst & Young LLP. (September 2017). Measuring Digital Advertising Revenue to Infringing Sites: TAG US Benchmarking Study. Retrieved from https://www.tagtoday.net/piracy/measuringdigitaladrevenuetoinfringingsites.

When research uncovered the full extent of criminal activity that had infiltrated the legitimate digital advertising supply chain, the entire industry jumped into action to achieve a healthier, cleaner ecosystem through the creation and support of TAG. Advertising networks and exchanges – the third parties that could potentially benefit from fraudulently inflated traffic rates – were among the earliest supporters of TAG. The recognition that legitimate companies benefit long-term from a cleaner, healthier ecosystem has driven more than 680 companies to apply for TAG membership. Furthermore, the TAG membership includes companies from every sector of the digital supply chain – from marketers and agencies, to ad tech firms and web publishers – and extends across 27 countries and 6 continents.

TAG's efforts also benefit from collaboration with Federal law enforcement. We have formed information-sharing partnerships with the Department of Homeland Security's Intellectual Property Rights Center and the Federal Bureau of Investigation's Cybercrimes and Financial Crimes Divisions. TAG also serves as the first Information Sharing and Analysis Organization ("ISAO") for the digital advertising industry to register with the ISAO Standards Organization, a non-governmental organization established by Congress to strengthen the nation's cybersecurity defense through information sharing. As the only ISAO for the digital ad industry, TAG serves as the lead information sharing organization around threats, incidents, and best practices, particularly those related to ad-related malware, ad-supported piracy, ad fraud and associated threats.

This culture of collaboration has always existed within our industry. In 2006, the Digital Advertising Alliance ("DAA") was established to promote more responsible privacy practices across the industry for relevant digital advertising, providing consumers with enhanced transparency and control through multifaceted principles that apply to multi-site data and cross-

app data gathered in either desktop, mobile web, or mobile app environments. The DAA is an independent non-profit organization led by leading advertising and marketing trade associations.

More recently, the leading international trade associations and companies involved in online media formed the Coalition for Better Ads ("CBA") to improve consumers' experience with online advertising. CBA leverages consumer insights and cross-industry expertise to develop and implement new global standards for online advertising that address consumer expectations.

V. Conclusion

TAG appreciates the Subcommittee's interest in helping Congress and the public better understand the digital advertising ecosystem. The digital advertising industry is one of the key drivers of the U.S. economy, empowering companies large and small. Although serious challenges face this vital industry, companies have rallied together to create effective self-regulatory solutions. I look forward to answering any questions that you may have.

Mr. LATTA. Well, thank you very much for your testimony.
Mr. Brookman, you are recognized for 5 minutes. Thank you.

STATEMENT OF JUSTIN BROOKMAN

Mr. BROOKMAN. Chairman Latta, Ranking Member Schakowsky, members of the committee, thank you very much for holding this hearing into the digital ad ecosystem and for the opportunity to testify here today.

I am here today on behalf of Consumers Union. We are the advocacy division of Consumer Reports. We are the world's largest independent testing organization, rating thousands of products and services for consumers every year.

I've been working on ad tech for a number of years now, dating back to suing adware companies in the 2000s for deceptive install practices.

I recognize the value of ad targeting. I also recognize that a lot of consumers really don't like it and they don't feel they've agreed to be tracked everywhere they go with everything they do in exchange for free content.

It used to be that online ad tracking was fairly straightforward. A lot of people didn't like it but it was simpler to understand. Advertising companies would put anonymous cookies in your browser and they serve you ads based on the sites you visited in your browser but not based on who you are, and you can control it by deleting or blocking cookies.

Today, however, the techniques companies use are a lot more sophisticated. Companies like Google and Facebook track you by real name, not just on their own services but on the majority of other sites and apps that are out there across all of your different devices.

Deleting cookies or using private browsing mode may not do much good anymore if companies are using other technologies like digital fingerprinting to monitor you instead.

And we are not just tracked on our computers anymore. It's other devices as well. Consumer Reports looked at a bunch of smart TVs earlier this year and all of them tried to use automated content recognition to take snapshots of what was on our screens to try to figure out what shows we are watching.

Ad companies also want to tie what we do online to the physical world. So a couple days ago I was in New York City. I bought a cup of coffee at a place I would never been before.

A day or so later, I got an email from them welcoming me to their rewards program. I had never given them my email address.

Now, I can see why companies might want to do some of these things but I also see why consumers might want to make it stop. Privacy is, at some level, a right to seclusion—a right to be left alone—a right to autonomy over our own devices and what they share about us, and it's getting harder and harder to manage that personal information.

Now, in response to this constant creeping encroachment into our personal spaces, there are some companies who are pushing back. Apple, for example, has done a lot to limit tracking and apps on iPhones. Just this week, they announced further changes to give users more control over cross-site tracking.

Mozilla, maker of the Firefox browser, has also taken a lot of positive steps to limit tracking in their browsers, and we've also seen a tremendous rise in the use of ad blockers like Disconnect and Privacy Badger and uBlock and Brave by consumers who are frustrated by aggressive ads or the underlying tracking.

Ad blocker penetration is expected to rise to 30 percent of the market this year, showing that users really are not satisfied with online ads' ecosystem.

In my organization, Consumer Reports—long-time testing lab—we are starting to test products based on privacy and security in response to consumer demand.

So I mentioned how we analyse privacy and security issues with TVs earlier. We are looking to build those sorts of evaluations into our everyday product testing.

And so far, though, all this pressure hasn't really been enough to get industry to reform itself. There are self-regulatory programs but they've always suffered from the same problems—they're too weak, they don't apply to all the companies in the space, they don't really address the data collection issue, the interfaces can be complicated and confusing, and a lot of times the tools are just broken.

Now, the online ad industry had agreed to address these failings back in 2012 when they promised to honor do not track instructions in browsers. These are the easy-to-use settings in your web browser. You can signal to the world that you don't want to be targeted and tracked.

Well, then a couple of years later the industry backtracked on that promise. Now it's been over 7 years since consumers have been activating do-not-track in their browsers. The ad industry still by and large just ignores those signals.

And so while we at Consumer Reports are working to improve the market for privacy and security, ultimately, I do think we probably need some basic legislative protections.

So we should have a discussion about what would work and what wouldn't, because privacy laws are already happening around the world.

Europe recently expanded their legal protections with the GDPR that just went into effect and a lot of other nations around the world are copying European models and those laws do affect U.S. companies.

States continue to pass privacy and security laws. States led the way on data breach notification laws and credit freeze laws and a lot of other basic consumer rights. We are starting to see them advance more comprehensive privacy and security legislation as well.

So I would urge this committee not to leave the policy decisions entirely to Europe or to the States but to really dig in and think about what sort of practical protections can empower consumers to make their own decisions about their personal information.

Thank you, again, for inviting me here today and I look forward to your questions.

[The prepared statement of Mr. Brookman follows:]

ConsumersUnion®
THE ADVOCACY DIVISION OF CONSUMER REPORTS

Statement of **Justin Brookman**
Director, Privacy and Technology Policy
Consumers Union

Before the House Subcommittee on Digital Commerce and Consumer Protection

Understanding the Digital Advertising Ecosystem

June 14, 2018

On behalf of Consumers Union, I want to thank you for the opportunity to testify today. We appreciate the leadership of Chairman Latta and Ranking Member Schakowsky in holding today's hearing to explore the digital advertising ecosystem and how digital advertisements affect Americans.

I appear here today on behalf of Consumers Union, the advocacy division of Consumer Reports, an independent, nonprofit, organization that works side by side with consumers to create a fairer, safer, and healthier world.[1]

[1] Consumer Reports is the world's largest independent product-testing organization. It conducts its advocacy work in the areas of privacy, telecommunications, financial services, food and product safety, health care, among other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million members and publishes its magazine, website, and other publications.

Executive Summary

My testimony today is divided into three parts. First, I describe some of the many ways that the digital advertising ecosystem has gotten more complex in recent years, leaving consumers with little information or agency over how to safeguard their privacy. Consumers are no longer just tracked through cookies in a web browser: instead, companies are developing a range of novel techniques to monitor online behavior and to tie that to what consumers do on other devices and in the physical world. Next, I discuss industry adjustments in the face of rising consumer pressure, including Consumer Reports' own efforts to provide more accountability for and transparency of individual company practices. While some companies have reformed their offerings in response to consumer privacy concerns, ad tracking companies have by and large taken advantage of opacity and consumer confusion to evade scrutiny — and have backtracked from prior commitments to offer better protections. Finally, I conclude by recommending that this Committee consider practical legislative steps to give consumers better rights over their personal data and digital security. Consumers want more and better privacy protections, but do not have the practical ability to take action. Congress should explore various options to give individuals the protections they want and deserve.

I. Ad Tracking Has Become More and More Invasive

In recent years, ad tracking technologies have become incredibly sophisticated, with consumers monitored in a variety of ways they can neither detect nor control. Online tracking is no longer limited to "anonymous" cookies that monitor a web browser from site to site. Modern advertising companies track users by their real name, across multiple computers, and increasingly across other internet-connected devices and into the physical world.

In describing these evolving tracking practices, I do not mean to imply that they are universally bad methods, or that they should all be prohibited. But understanding the proliferation of tracking behaviors puts into context how increasingly difficult it is for individuals to exercise control over their personal information. Consumers are actively engaged online, spending around six hours per a day using digital media, mostly on mobile devices.[2] While some consumers may well appreciate receiving targeted offers, in study after study, the majority of people do not wish to be tracked in order to be served with more relevant advertising.[3] In a recent Pew Research study, 86% of users reported taking some action to mask their digital footprints, but most wish they had the ability to do more.[4] Older, less tech-savvy users especially feel powerless to take responsibility of protecting their privacy.[5] In the past, simply blocking cookies may have been sufficient to prevent the sort of online tracking that many consumers reject. Today, tracking takes many more

---

[2] Ginny Marvin, *Digital Advertising's Opportunities & Threats from Mary Meeker's Internet Trends Report*, MARKETING LAND (June 1, 2018), https://marketingland.com/digital-advertisings-opportunities-threats-from-mary-meekers-internet-trends-report-241264.

[3] Chris Jay Hoofnagle et al., *Privacy And Modern Advertising: Most US Internet Users Want 'Do Not Track' to Stop Collection Of Data About Their Online Activities*, AMSTERDAM PRIVACY CONFERENCE (Oct. 8, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152135; Kristin Purcell et al., *Search Engine Use Over Time*, PEW RESEARCH CTR. (Mar. 9, 2012), http://www.pewinternet.org/2012/03/09/main-findings-11/; J. Turow et al., *Americans Reject Tailored Advertising And Three Activities That Enable It,* SSRN (2009), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[4] Lee Raine, *The State of Privacy In Post-Snowden America*, PEW RESEARCH CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

[5] Fatemeh Khatibloo, *Marketers, Here's How Your Customers Feel About Privacy*, FORBES (Dec. 16, 2016), https://www.forbes.com/sites/forrester/2016/12/16/marketers-heres-how-your-customers-feel-about-privacy/#52356c0f18e4.

forms, and is increasingly difficult to limit or control.

A. Real Name Tracking

Advertising companies previously defended online tracking because it was "anonymous" — digital companies didn't care *who* you were, they just wanted to market relevant products to unidentified users. In 2001, the Federal Trade Commission (FTC) closed an investigation into DoubleClick's merger with the data broker Abacus noting that: "DoubleClick did not combine PII [personally identifiable information] from Abacus Direct with clickstream collected on client Web sites."[6] Further, in 2008, in describing its "Commitment to Privacy in Online Advertising" to the U.S. Senate Commerce Committee, Microsoft explained that it relied on a de-identification process "to ensure that we use only data that does not personally identify individual consumers to serve ads online."[7]

Today, however, online tracking is no longer anonymous. In 2010, Facebook made available to publishers its now-ubiquitous "Like" buttons to embed into their web pages.[8] Because those buttons connect to Facebook directly even without any user interaction, Facebook is able to track registered users off of Facebook by their real names.[9] A recent study of leading websites determined that Facebook is embedded in approximately 69% of the those sites, giving Facebook broad insight into what people do off of their services.[10] Beginning in 2015, Facebook started to

---

[6] *Letter to DoubleClick*, FED. TRADE COMM'N (Jan. 22, 2001), https://www.ftc.gov/sites/default/files/documents/closing_letters/doubleclick-inc./doubleclick.pdf.
[7] *Statement of Michael D. Hintze, Before the U.S. Senate Comm. On Commerce, Sci. & Transp.*, MICROSOFT CORP., 15 (Jul. 9, 2008), available at https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00020/544506-00020.pdf.
[8] Tom Simonite, *Facebook's Like Buttons Will Soon Track Your Web Browsing to Target Ads*, MIT TECH REV. (Sept. 16, 2015), https://www.technologyreview.com/s/541351/facebooks-like-buttons-will-soon-track-your-web-browsing-to-target-ads/.
[9] Allen St. John, *How Facebook Tracks You, Even When You're Not on Facebook*, CONSUMER REPORTS (Apr. 11, 2018), https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook/.
[10] Justin Brookman et al., *Cross-Device Tracking: Measurement and Disclosures*, PROCEEDINGS ON PRIVACY ENHANCING TECH. (2017), *available at* https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf.

use this data for ad targeting: thus, if Facebook tracked your shopping cart on a oline shoe seller site, it could later serve you an ad for shoes on Facebook (or possibly on a different site).[11] In 2016, Google followed suit and merged its logged-in user data with its third-party advertising data; for users who have signed into products such as Gmail or YouTube,

Google can now combine behavioral data collected off of Google through DoubleClick and other products with real name identity.[12] Google's penetration of the web is even greater than Facebook, appearing in over 87% of surveyed sites in one study.[13]

B. Cross-Device Tracking

Users typically log into Google and Facebook on different devices. As a result, those companies are able to monitor what you do around the web and in other apps on multiple devices — and to link all of that behavior together, tied to your identity.[14]

Other ad tracking companies may not have easy access to identifying information, but they increasingly use a variety of other tactics to try to correlate user behavior across different devices. Some many use *probabilistic* methods to identify devices that may share an owner based on shared attributes, such as internet protocol address. If two devices generally connect to the same local network, there is a decent chance they are used by the same individual. If they also exhibit similar browsing patterns (for example, the user on both devices tends to visit sites about the Washington

---

[11] *See Facebook's Like Buttons*, *supra* note 8.
[12] Julia Angwin, *Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking*, PROPUBLICA (Oct. 21, 2016), https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking.
[13] See *Cross-Device Tracking*, *supra* note 10. For a more extensive look at tracking on over one million of the top sites, *see* Steven Englehardt & Arvind Narayanan, *Online Tracking: A 1-Million-Site Measurement and Analysis*, PRINCETON WEB CENSUS (2016), http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf; Russell Brandom, *Google And Facebook Still Dominate Tracking on The Web*, THE VERGE (May 18, 2016), https://www.theverge.com/2016/5/18/11692228/google-facebook-web-tracking-survey-advertising.
[14] *See Cross-Device Tracking: An FTC Report*, FED. TRADE COMM'N, 2-3 (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.

Capitals and technology law), they are even more likely to share an owner.[15]

Some companies receive identifying information from publishers that collect login information. If you provide your email address or username to a website to log into a service, that service may share that identifying information with various ad tracking companies. If a tracking company receives the same identifiers across multiple devices, it is able to generate a *deterministic* cross-device profile of the user.[16]

Furthermore, some companies have experimented with other technologies such as ultrasonic audio beacons to track users across devices. Audio beacons are inaudible signals that are played through a speaker on a connected device like a computer, tablet, or TV. If an ultrasonic code is played in the vicinity of a device that has software in an app or other platform that can listen for the inaudible code, the listening device will then identify that the same individual has used both devices and thereby enable an advertiser to more accurately track a user across devices.[17] Advertisers have also embedded software in apps that would enable companies to know what a user is watching on their TV by listening through the device's microphone. This information can then be added to a profile about a user and used to create targeted advertisements for the individual. In early 2016, the FTC issued warning letters to developers who installed audio beacon software in apps in order to listen for inaudible signals to log what users watched on TV.[18] Despite this warning, other developers like Alphonso have continued to make use of similar technologies in order to track users across different devices and served targeted ads.[19]

---

[15] *Id.* at 3.
[16] For a more detailed discussion of these methods, *see, generally, Cross-Device Tracking, supra* note 8.
[17] *Comments for November 2015 Workshop on Cross-Device Tracking*, CTR. FOR DEMOCRACY & TECH. (Oct. 16, 2015), https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf.
[18] *FTC Issues Warning Letters to App Developers Using 'Silverpush' Code*, FED. TRADE COMM'N (Mar. 17, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code.
[19] Sapna Maheshwari, *That Game on Your Phone May Be Tracking What You're Watching On TV*, N.Y. TIMES (Dec. 28, 2017), https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html. According to

C. Internet of Things

More and more of the objects we use and purchase are technology- and internet-enabled. Cars, televisions, home assistants, and even kitchen appliances have the ability to go online to expand the functionality of those products. At the same time, ad tracking companies can leverage the information generated by these devices to expand a marketing profile about a user — often without a great deal of transparency.

Smart televisions are a good example. Many smart TVs use a technology called "automated content recognition" (ACR) to collect and transmit screenshots from the TV in order to determine what types of content the household is watching. In 2015, the FTC reached a settlement with the manufacturer Vizio over its use of ACR to track the television viewing habits of consumers without clear permission.[20] Consumer Reports published the results of its own investigation of smart TV behavior earlier this year, finding that all the major TV manufacturers examined used ACR to monitor owners' use of their products (with varying degrees of transparency and control).[21]

Voice assistants in the home like Amazon's Echo, Sonos's One, and Google's Home present further possibilities for tracking, though advertisers have not fully realized the opportunity to reach consumers via these new sources yet.[22] Adoption of these devices is expected to reach the

---

the *New York Times* report, Alphonso used a different type of technology in order to determine what shows users were listening, similar to the automated content recognition described in the following section used by smart televisions.

[20] *Vizio to Pay $2.2 Million to FTC, State of New Jersey To Settle Charges It Collected Viewing Histories On 11 Million Smart Televisions Without Users' Consent*, FED. TRADE COMM'N (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

[21] *Samsung And Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds*, CONSUMER REPORTS (Feb. 7, 2018), https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/. The *Consumer Reports* study also found security vulnerabilities in two of the televisions that would allow hackers to manipulate the television remotely to, for example, set the volume to maximum, or display offensive content.

[22] *See Digital Advertising's Opportunities*, *supra* note 2.

majority (55%) of all U.S. households by 2022.[23] These devices may well expand data collection capacity and facilitate the delivery of targeted advertisements. Advertising through voice assistants would also present additional challenges to transparency, as consumers will not have visual indicators that particular recommendations are paid advertisements and may have less opportunity to learn about and control the way their data is collected and used.

D. The Constant Proliferation of Tracking Technologies

The methods described above are just a subset of some of the new tactics that companies use to track and target consumers. But the list is far from exhaustive. Other examples include: tailoring of online ads based on in-store purchases,[24] the collection of cell phone signals to generate in-store retail analytics,[25] internet service provider monitoring of user behavior for ad targeting,[26] and email targeting based simply on visiting a website[27] or making a purchase at a retail location.[28] Academic researchers at institutions such as Princeton, Northeastern, and the University of California have researched and cataloged many of these behaviors,[29] but it is next to impossible

[23] Sarah Perez, *Voice-Enabled Smart Speakers to Reach 55% Of U.S. Households By 2022, Says Report*, TECHCRUNCH (Nov. 8, 2017), https://techcrunch.com/2017/11/08/voice-enabled-smart-speakers-to-reach-55-of-u-s-households-by-2022-says-report/.
[24] Tim Peterson, *Facebook Will Target Ads to People Based on Store Visits, Offline Purchases, Calls to Businesses*, MARKETING LAND (Sept. 21, 2017), https://marketingland.com/facebook-will-target-ads-people-based-store-visits-offline-purchases-calls-businesses-224668.
[25] Siraj Datoo, *How Tracking Customers In-Store Will Soon Be the Norm*, THE GUARDIAN (Jan. 10, 2014) https://www.theguardian.com/technology/datablog/2014/jan/10/how-tracking-customers-in-store-will-soon-be-the-norm.
[26] Jon Brodkin, *How ISPs Can Sell Your Web History—And How to Stop Them*, ARS TECHNICA (Mar. 24, 2017), https://arstechnica.com/information-technology/2017/03/how-isps-can-sell-your-web-history-and-how-to-stop-them/
[27] Jess Nelson, *Criteo Launches Dynamic Email Retargeting Solution*, MEDIAPOST (May 20, 2016) https://www.mediapost.com/publications/article/276266/criteo-launches-dynamic-email-retargeting-solution.html.
[28] Ben Popper, *Square Adds Marketing Tools So Merchants Can Email Their Customers*, THE VERGE (Apr. 7, 2015), https://www.theverge.com/2015/4/7/8359483/square-marketing-email-promotions.
[29] *See, e.g.*, PRINCETON WEB TRANSPARENCY AND ACCOUNTABILITY PROJECT, https://webtap.princeton.edu/ (last visited June 12, 2018). For the past three years, the Federal Trade Commission has held *PrivacyCon* to hear from cutting edge privacy researchers in order to educate itself and the policy community about some of these latest tracking techniques. *See* FED. TRADE COMM'N'S PRIVACYCON 2018 (last visited June 12, 2018), https://www.ftc.gov/news-events/events-calendar/2018/02/privacycon-2018.

for ordinary consumers to learn about how they are being monitored, or take control of their personal information. Indeed, many privacy violations are completely unobservable by consumers. For instance, if personal data stored with a cloud provider is transmitted to someone else, consumers have no visibility into that transmission. If the data is accessed inadvertently or maliciously, the provider may have obligations to disclose to consumers under breach notification laws. However, if the transmission is intentional — that is, if the provider deliberately provides data to a third-party — a consumer would have no way to detect that disclosure of their information.

Persistent confusion — even among experts — about whether and how connected products and services can listen to personal conversations illustrates the challenges for consumers.[30] Just last week, Vice published a story purporting to prove that Facebook listens to ambient conversations for ad targeting purposes.[31] Privacy researchers cast doubt on the story, but the fact that leading authorities cannot even agree on whether Facebook is mining personal audio conversations is emblematic of the generalized confusion about privacy in a world of connected sensors. When sophisticated technology reporters cannot figure out how their personal information is collected and used,[32] the challenge for average consumers — worried about privacy but without the time or training to protect themselves — becomes clear. And the public is left feeling frustrated and helpless.

---

[30] David Goldman, *Your Samsung TV Is Eavesdropping on Your Private Conversations*, CNN (Feb. 10, 2015), http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/index.html.
[31] Sam Nichols, *Your Phone Is Listening and It's Not Paranoia*, VICE (June 4, 2018), https://www.vice.com/en_uk/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia.
[32] *See, e.g.*, Kashmir Hill, *Facebook Figured Out My Family Secrets and It Won't Tell Me How*, GIZMODO (Aug. 25, 2017), https://gizmodo.com/facebook-figured-out-my-family-secrets-and-it-wont-tel-1797696163; JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE (2014).

II. Some Companies are Responding to Market Pressure, but Industry Self-Regulation Has Failed to Date

Unfortunately, digital advertising is still largely opaque to the consumer who is tracked both on- and off-line. Consumers feel like they lack control over how often their personal information is shared and how much digital advertisers know about them.

In response to these concerns, some market actors have made significant changes to limit data collection on their platforms. For example, Apple, in 2013 introduced a mandatory "Limit Ad Tracking" setting for iPhone applications, and recently improved that tool to further limit the information advertisers can receive when the setting is activated.[33] Mozilla too has taken efforts to differentiate its Firefox web browser by adopting policies to limit cross-site data collection.[34] Services like DuckDuckGo have found some success in marketing themselves as the tracking-free alternative to larger search engine companies that rely on data for advertising.[35] And a number of private entities have developed ad blockers that stop many online tracking techniques, such as Disconnect.me, the Electronic Future Foundation's Privacy Badger, and uBlock. Industry analysts expect ad blocker adoption to reach 30% this year, led primarily by the youngest internet users.[36] The start-up Brave has also developed browsers that block ads by default, and is exploring alternative web funding models based on privacy-friendly ads and micropayments of cryptocurrency.[37]

---

[33] Lara O'Reilly, *Apple's Latest iPhone Software Update Will Make It A Lot Harder for Advertisers to Track You*, BUS. INSIDER (Sept. 10, 2016), http://www.businessinsider.com/apple-ios10-limit-ad-tracking-setting-2016-9.
[34] Monica Chin, *Firefox's Quantum update will block websites from tracking you 24/7*, MASHABLE (Jan. 23, 2018), https://mashable.com/2018/01/23/firefox-quantum-releases-update/#yPrZ0O74MqqQ.
[35] Apekshita Varshney, *Hey Google, DuckDuckGo Reached 25 Million Daily Searches*, TECHWEEK (June 4, 2018), https://techweek.com/search-startup-duckduckgo-philadelphia/.
[36] *30% of All Internet Users Will Ad Block By 2018*, BUS. INSIDER (Mar. 21, 2017), http://www.businessinsider.com/30-of-all-internet-users-will-ad-block-by-2018-2017-3.
[37] Stephen Shankland, *Ad-Blocking Brave Browser to Give Crypto-Payment Tokens to Everyone*, CNET (Apr. 19, 2018), https://www.cnet.com/news/ad-blocking-brave-browser-to-give-crypto-payment-tokens-to-everyone/.

For its part, Consumer Reports is taking steps to provide more accountability for the market and to give consumers actionable information about which companies do a better job of protecting user privacy. To help consumers make decisions in the marketplace, Consumer Reports has developed, and is actively testing products under, the Digital Standard. The Digital Standard[38] is an open standard for testing products and services for privacy and security. Our testing under the Standard includes assessments of a company's stated privacy practices in both the user interfaces and in their privacy policies, as well as analysis of traffic flows. And it examines such questions as: Does the company tell the consumer what information it collects? Does it only collect information needed to make the product or service work correctly? And does the company explicitly disclose every way it uses the individual's data?[39] While we are currently conducting case studies under the Standard to ensure that the process is scientific and repeatable, we plan to eventually include privacy and digital security in our comparative testing of products where there is potential market differentiation. Our ultimate goal is to enable consumers to make better, more informed privacy choices, and to spur improvements and greater competition among companies on privacy.

Despite some market improvements, as discussed above, tracking technology has gotten more invasive in recent years. Moreover, industry efforts to self-regulate have largely failed. Five years ago, I testified about the various weaknesses in ad tracking self-regulatory programs: the rules only apply to coalition members; industry opt-outs are fragile and easily overridden; industry opt-outs only address usage and do not impose meaningful collection or retention limitations; and

---

[38] The Digital Standard (theDigitalStandard.org) was launched on March 6, 2017 and is the result of a collaboration with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use everyday.

[39] *Id.*

notice and privacy interfaces were seriously flawed.[40] These criticisms largely remain intact today, before even considering the dramatic expansion of tracking technologies in recent years.

Industry had originally committed to addressing these flaws by adopting the Do Not Track web standard to give consumers a more robust opt-out tool. In 2012, industry representatives committed to honoring Do Not Track instructions at a White House privacy event.[41] Over the next few years, however, as regulatory pressure and the prospect of new legislation faded, industry backed away from its commitment, with trade groups publicly announcing withdrawal from the industry standard process at the World Wide Web Consortium.[42] Today, seven years after Do Not Track settings were introduced into all the major browser vendors, few ad tracking companies meaningfully limit their collection, use, or retention of consumer data in response to consumers' Do Not Track instructions.

III. American Consumers Deserve Stronger Privacy Rights Under the Law

Consumers Union and Consumer Reports are committed to improving transparency and incentivizing the market to sufficiently protect personal information through product testing under the Digital Standard. However, ultimately, U.S. consumers need stronger privacy laws to give users greater rights and protections in a world of universal surveillance and connectivity.[43] Such a law should require:

---

[40] *Statement of Justin Brookman Before the U.S. Senate Comm. On Commerce, Sci., and Transp.*, CTR. FOR DEMOCRACY & TECH. (Apr. 24, 2013), https://cdt.org/files/pdfs/Brookman-DNT-Testimony.pdf.
[41] Dawn Chmieleski, *How 'Do Not Track' Ended Up Going Nowhere*, RECODE (Jan. 4, 2016), https://arstechnica.com/information-technology/2017/03/how-isps-can-sell-your-web-history-and-how-to-stop-them/; *see* Julia Angwin, *Web Firms to Adopt 'No Track' Button*, WALL ST. J. (Feb. 23, 2012), https://www.wsj.com/articles/SB10001424052970203960804577239774264364692.
[42] Kate Kaye, *Do-Not-Track on The Ropes as Ad Industry Ditches W3C*, ADAGE (Sept. 17, 2013), http://adage.com/article/privacy-and-regulation/ad-industry-ditches-track-group/244200/.
[43] Jessica Rich, *Beyond Facebook, It's High Time for Stronger Privacy Laws*, WIRED (Apr. 8, 2018), https://www.wired.com/story/beyond-facebook-its-high-time-for-stronger-privacy-laws/.

- Clear, easy-to-understand and compare information about data practices;
- Simple and easy-to-use consumers choices;
- The collection and retention of only the data necessary — and the disposal of old data;
- Strong data security practices;
- Ways for consumers to get easy access to their information; and
- A strong enforcement cop to ensure accountability.[44]

Unfortunately, legal protections at the federal level are — if anything — getting weaker.[45] Just last week, an appeals court further constrained the FTC's already limited authority to order companies to cease bad data security practices.[46] Currently, it is the states that are advancing legislation to safeguard consumer privacy and security. For example, a ballot initiative in California this November may establish mandatory transparency and opt-out requirements around the sale of personal information to third-party data brokers.[47] Just as states have determined the legal landscape for data breach notification,[48] states seem poised to set more comprehensive standards for security and data privacy. While Consumers Union supports many of these state legislative initiatives, a strong, consistent federal law ensuring privacy and security protections for all personal data is still needed. We urge this Committee to hold further hearings on this issue, with a focus on how legislation can balance individual liberty and agency with the need to account for future technologies and innovation.

---

[44] *Where We Stand: Congress Should Pass A Strong Privacy Law, Now*, CONSUMER REPORTS (Apr. 9, 2018), https://www.consumerreports.org/privacy/its-time-for-congress-to-pass-a-strong-privacy-law/.
[45] Justin Brookman, *Protecting Privacy in An Era of Weakening Regulation*, HARV. L. & POL'Y REV., Vol. 9 (2015), *available at* http://harvardlpr.com/wp-content/uploads/2015/07/9.2_3_Brookman.pdf.
[46] Alison Frankel, *There's A Big Problem for The FTC Lurking in the 11th Circuit's LabMD Data-Security Ruling*, REUTERS (June 7, 2018), https://www.reuters.com/article/us-otc-labmd/theres-a-big-problem-for-the-ftc-lurking-in-11th-circuits-labmd-data-security-ruling-idUSKCN1J32S2.
[47] Daisuke Wakabayaski, *Silicon Valley Faces Regulatory Fight on Its Home Turf*, N.Y. TIMES (May 13, 2018), https://www.nytimes.com/2018/05/13/business/california-data-privacy-ballot-measure.html.
[48] *Data Breach Notification Laws: Now in All 50 States*, PRIVACY RIGHTS CLEARINGHOUSE (May 9, 2018), https://www.privacyrights.org/blog/data-breach-notification-laws-now-all-50-states.

Conclusion

Thank you again for the opportunity to testify here today about the state of the digital advertising marketplace and the need for strong consumer controls over how their data is collected and used. I look forward to answering the Committee's questions.

Mr. LATTA. Well, thank you again for your testimony.
And Dr. Beales, you are recognized for 5 minutes. Thank you.

STATEMENT OF J. HOWARD BEALES III

Dr. BEALES. Thank you, Chairman Latta, Ranking Member Schakowsky, and members of the subcommittee. I thank you for the opportunity to testify today.

I am Howard Beales. I am a professor of strategic management and public policy at the George Washington School of Business. I've written academic articles about privacy and from 2001 to 2004 I was the director of the Bureau of Consumer Protection at the FTC at the time when the commission promulgated the National Do Not Call Registry.

I want to make three essential points this morning. First, internet content is a public good. Private market provisions of such public goods has historically depended on revenue from advertising, as does internet content today.

Second, the value of advertising depends critically on the availability of information about the likely viewer. When information is available, advertising prices are, roughly, three times higher than when there's no information about the viewer.

Impairing the flow of information would significantly reduce the revenues available to support internet content, an impact that would be particularly problematic for smaller publishers.

Third, advertising actually benefits consumers, leading to more competitive markets, lower prices, product improvements, and smaller differences between demographic groups.

To return to my first point, from an economic perspective, internet content is a public good. Unlike private goods, public goods are not used up in consumption.

Like free broadcast radio or television, any number of consumers can enjoy the content without any additional cost of providing it. The primary market mechanism for providing such goods is advertising, which converts the public good of media content into a private good of exposures to advertising.

Throughout history, advertising support has been a vital revenue source for media companies. Although purer subscription models exist, like satellite radio or premium cable TV, market behavior makes clear that most consumers most of the time are not willing to pay a premium price to avoid advertising.

Online content is not fundamentally different. Publishers must cover their costs and advertising is critical to achieve that objective. Given the long histories of advertiser-supported media markets, that fact should not be surprising and it's not likely to change.

Second, the value of advertising depends on information. What advertisers are willing to pay for an advertising slot depends critically on what they know about the viewer. However attractive to an individual viewer, anonymity reduces the price of the advertisement and therefore reduces the revenue available to support the content the viewer is enjoying.

In short, anonymity is a subtle form of free riding on the contributions of others. In two separate studies I've examined the impact of better information on the price of digital advertising.

In a 2010 study, I surveyed advertising networks to determine the impact of behavioral targeting which uses browsing behavior data to categorize likely consumer interest in a particular advertisement.

The price for behaviorally targeted advertising was, roughly, three times higher than the price of run of network advertising sold without regard to audience characteristics, and that's a substantial prices premium.

My 2013 study analysed data from automated advertising exchanges. If there was a cookie available, the price of the advertisement was, roughly, three times higher than if there was no cookie. The longer the cookie had been in place, the more it was worth. With a 90-day-old cookie, the price was between 3.7 and 7.1 times higher than the price with no cookie.

We also found that even the largest publishers sold about half of their ad slots through third-party technologies like ad exchanges while smaller long-tail publishers relied on these approaches for up to two-thirds of their advertising sales.

Thus, regulatory requirements that impair the flow of information will significantly reduce the revenue available to online content producers, leading to a less vibrant internet. The impact will be greatest on the smallest publishers.

Many important participants in the online marketplace are not consumer facing at all because they work with publishers or advertisers to observe behavior across independent websites.

Consumers have never heard of most of them: for example, 33Across, Accuen, Acuity, and Adara, which happen to be the first four names on the list of members of the Network Advertising Initiative.

More elaborate consent requirements could seriously disadvantage these companies with the primary effect of protecting the market shares of the current leaders in the online advertising market.

As in any other market, regulatory barriers that protect market leaders from competition are bad for consumers.

Finally, advertising is not evil. It provides important benefits for consumers. Numerous economic studies have shown that restrictions on advertising increase prices for consumers.

Advertising also facilitates innovation and narrows the differences between demographic groups. Advertising the relationship between fiber consumption and cancer, for example, resulted in the greatest increases in fiber consumption in racial minority and single parent households.

When eyeglass advertising was restricted, the least educated paid the highest prices.

To summarize, the provision of internet content depends on advertising revenue. That revenue, in turn, depends on the availability of information about the viewer, and online advertising, like other advertising, benefits consumers.

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

[The prepared statement of Dr. Beales follows:]

Testimony of

J. Howard Beales III
Professor of Strategic Management and Public Policy
George Washington School of Business

Before the

Subcommittee on Digital Commerce and Consumer Protection
Committee on Energy and Commerce
House of Representatives

On

Understanding the Digital Advertising Ecosystem

June 14, 2018

Chairman Latta. Ranking member Schakowsky, and members of the subcommittee, thank you for the opportunity to testify today on the Digital Advertising Ecosystem. I am Howard Beales, a Professor of Strategic Management and Public Policy at the George Washington School of Business. I have published a number of academic articles on privacy regulation. From 2001 to 2004, I was the Director of the Bureau of Consumer Protection. During that time, the Commission re-thought its approach to privacy regulation and promulgated the National Do Not Call Registry.

I want to make three essential points this morning. First, internet content is a public good: it is not used up in consumption. Private market provision of such public goods has generally depended on revenue from advertising, as does internet content today. Second, the value of advertising depends critically on the availability of information about the likely viewer. When information is available, advertising prices are roughly 3 times higher than when there is no information about the viewer. Impairing the flow of information would significantly reduce the revenues available to support internet content, an impact that would be particularly problematic for smaller publishers. Third, advertising is actually beneficial to consumers. It leads to more competitive markets, with lower prices and more product improvements. It also narrows the differences between different demographic groups.

Internet Content is a Public Good

The Internet has allowed an unprecedented diffusion of information to consumers. Among a nearly infinite variety of possibilities, consumers can now listen to radio broadcasts, watch television programs, read the daily paper, or just hang out with their friends online. Although these activities have considerable value to consumers, they are frequently supplied to

consumers free of charge. Instead, Internet content is largely funded by advertisers who pay to have their ads included along with the online content.

From an economic perspective, Internet content is a "public good." Unlike private goods, public goods are not "used up" in consumption, and instead remain available for other consumers to enjoy. A classic example of a public good is free broadcast radio or television. Any number of consumers can enjoy the content, without any additional costs of providing it.

Long before the Internet, publishers developed effective mechanisms to finance content that consumers wanted despite the public good nature of their product. Conventional media markets face the same underlying economic issues, and offer valuable insights into successful models for the provision of content.

The most common market mechanism for providing public goods is advertising. In effect, advertising converts the public good of media content into a private good of exposures to advertising. Content becomes a way for the publisher, to attract an audience that in turn can be sold to advertisers. Because advertisers ultimately want to reach individual consumers, a larger audience is more valuable than a smaller one – it produces more advertising exposures available for sale.

The business of producing content and selling advertising is a "two-sided" or "platform" market. Content must attract an audience, but the platform must also attract advertisers. The financial support for the content comes from advertising revenue. In some circumstances, such as directories or fashion magazines, advertising may increase the overall value of the product to consumers. In other circumstances, however, advertising is a nuisance: Too much advertising, or advertising that is too intrusive or offensive to consumers, may drive away some of the

audience, thereby reducing the number of advertising exposures that can be sold. The publisher must consider both sides of the market in deciding what content to provide and how much advertising to offer.

Throughout history, advertiser support has been a vital revenue source for media companies. Many, such as free broadcast radio or television, depend almost entirely on advertising revenue for survival. Also common are mixed models, such as the typical magazine or newspaper, or cable television programming, where subscription payments from consumers provide some revenue, but typically advertising revenue remains vital and is frequently the largest source of revenue.

There are, of course, some models that are purely supported by subscription revenues, such as satellite radio or premium cable TV channels. Market behavior makes clear, however, that most consumers most of the time are not willing to pay a premium price to avoid advertising content.

There is nothing fundamentally different in the provision of online content from providing similar content in conventional media markets. Publishers, ranging from major media companies to specialty sites that specialize in particular niches, must cover the costs of producing the content they provide. Although there are other models, by far the most common business model supporting the provision of Internet content is advertising. Given the long history of advertiser supported media markets, that fact should not be surprising.

The Value of Advertising Depends on Information

In any media market, the price of advertising depends on the characteristics of the audience. In conventional media, where large numbers of consumers of necessity see the same advertisement, advertisers choose where to advertise based on the demographic characteristics of the audience as a whole. Not surprisingly, some audiences are more valuable than others, because more advertisers are interested in reaching them or they are harder to attract to programming. Advertising prices therefore depend on audience demographics as well.

Online, each consumer who visits a website can be served a different advertisement. What advertisers are willing to pay for that slot, however, depends critically on what they know about the viewer. And in turn, what advertisers are willing to pay determines the resources available to support the content of that particular website. Anonymity may appear attractive to an individual viewer, but because it reduces the price of the advertisement, it reduces the revenue available to support the content of the website that the viewer is enjoying. It is, in short, a subtle form of free riding on the contributions of others.

There are two predominant forms of online advertising: search advertising and, broadly speaking, display advertising. Search advertising is purchased based on the keywords that a consumer has just entered in a search engine and is usually sold on a cost per click basis. That is, the web page is paid based on the number of clicks on the advertisement, rather than the number of consumers who see it. Advertisers bid for keywords, and the search engine provider will select which advertisements to include in the results based on the bid price and its own estimate of the likelihood that this consumer will find the advertisement sufficiently interesting to click on

it. Information that enables the search provider to make better estimates of the likelihood that a consumer will click on the link will increase the provider's revenue.

The other major category of online advertising is display advertising, which includes display and banner ads, rich media, and digital video ads. Display advertising is generally sold on a cost per thousand (CPM) basis. Third party intermediaries, including advertising networks and ad exchanges, are key participants in this marketplace. Advertising networks pool inventory from numerous, usually small publishers. Advertising is increasingly sold in real-time auctions, with advertisers bidding for particular advertising availabilities based on what, if anything, they know about the viewer. In the auction, the highest bidder wins the advertisement, at the price offered by the second highest bidder. Information about the viewer is obtained through cookies, which enable advertising networks and others to determine what other websites that particular user has visited.

In two separate studies, I have examined the impact of better information on the price of digital advertising. In a 2010 study, I surveyed 12 of the 15 largest advertising networks to determine the impact of behavioral targeting, which uses data based on user browsing behavior across multiple web sites to categorize likely consumer interest in a given advertisement. I compared the price of advertising on a CPM basis when it was sold based on behavioral targeting with the price when the advertisement was sold on a "run of network" basis, meaning that it could appear anywhere on the network with no specification as to the characteristics of the user. I found that the CPM for behaviorally targeted advertising was roughly 3 times higher than the

price of run of network advertising – a substantial price premium. I also found that the majority of advertising revenue was passed through to the publisher.1

A second study, with Jeffrey Eisenach, analyzed 2013 impression-level data from two anonymous operators of automated advertising exchanges to determine how better information influenced the auction price. We found that more information led to a price premium that was both statistically and economically significant. If there was a cookie available with the impression, the price was roughly 3 times higher than if there was no cookie. Moreover, the longer the cookie had been in place, the greater was the increase in price. The price of an impression with a cookie that had been in place for 90 days was 3.7 times higher than the price with no cookie on one exchange, and 7.1 times higher on the other. The study also used data from Adomic, which measured the relative prevalence of different advertising sales models across the top 4,000 Internet publishers. Even the largest publishers sold about half of their advertising availabilities through third-party technologies, while smaller, "long-tail" publishers relied on these approaches for up to two thirds of their advertising sales.2

Other studies support the same conclusion: the value of online advertising, and hence the revenue available to support the production and development of online content, depends critically on the availability of information about the likely viewer of the ad. Regulatory requirements that impair the flow of information will significantly reduce the revenue available

---

[1] Howard Beales, "The Value of Behavioral Targeting," published online by Network Advertising Initiative, available at http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf, March, 2010.

[2] J. Howard Beales and Jeffrey A. Eisenach, "An Empirical Analysis of the Value of Information Sharing in the Market for Online Content," published online by Digital Advertising Alliance, available at http://www.aboutads.info/resource/fullvalueinfostudy.pdf, January, 2014.

to online content producers, leading to a less vibrant Internet. The impact will be greatest on the smaller publishers, who are most dependent on third-party technologies for advertising revenue.

It is also vital to recognize that regulatory rules are likely to have very different impacts on different companies. Companies that utilize sign-ins are likely to have the most information, because they can typically observe the consumer's behavior whenever he or she is signed in to the service. Thus, Facebook and Google likely have significant informational advantages over other participants in the online advertising marketplace. Some large publishers with many different content pages will have information about behavior as the consumer moves around their various offerings. Other important participants in the online marketplace, however, are not consumer-facing at all. Instead, they work with publishers or advertisers to observe behavior across independent websites through the use of cookies. There are numerous such companies, most of whom consumers have never heard of – for example, 33across, Accuen, Acuity, and Adara, which happen to be the first four names on the the list of members of the Network Advertising Initiative. More elaborate consent requirements could seriously disadvantage these companies, and help protect the market shares of the current leaders in the online advertising market: Facebook and Google. As in many other areas, large players in online advertising markets have incentives to agree to regulatory requirements that they can satisfy more easily than their smaller competitors. And as in any other market, creating regulatory barriers that have the effect of protecting market leaders from competition is bad for consumers.

Advertising Provides Important Benefits for Consumers

Individually, we may think of advertising as a nuisance, and many times it is. The ability to advertise, however, is critical to maintaining effective competition in markets for goods and services.

The competitive benefits of advertising are by now well known. In the words of Nobel Laureate George Stigler, "advertising is an immensely powerful instrument for the elimination of ignorance."3 Informed consumers drive the competitive process, benefitting all consumers as sellers compete for the informed minority.4 Numerous economic studies have shown that restrictions on advertising increase prices to consumers, even when advertising does not mention price.5

Advertising also stimulates innovation. If sellers cannot advertise innovative products, or if they cannot tell consumers why new product characteristics are important, there is less incentive to make improvements in the first place.6 One of the best studied examples involves Kellogg's 1984 claims for All Bran cereal, conveying the then novel recommendation of the National Cancer Institute ("NCI") that diets high in fiber may reduce the risk of some cancers.7 The science, which was based largely on epidemiology rather than human clinical trials, was

---

3 George J. Stigler, The Economics of Information, 64 J. POL. ECON. 213, 220 (1961).

4 See, e.g., Alan Schwartz and Louis L. Wilde, Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis, 127 U. PA. L. REV. 630 (1978-1979).

5 The FTC itself has summarized the empirical evidence regarding the impact of advertising on prices. See In re Polygram, 2003 WL 21770765 (FTC), Docket No. 9298 (July 24, 2003), at note 52.

6 Advertising is an intangible investment, whose value can only be recovered through repeat sales. Sellers invest in and maintain product quality to generate repeat business. See Phillip Nelson, Advertising as Information, 82 J. POL. ECON. 729 (1974).

7 The Kellogg incident is discussed in J. Howard Beales, Timothy J. Muris, and Robert Pitofsky, "In Defense of the *Pfizer* Factors," in James C. Cooper, Ed., *The Regulatory Revolution at the FTC: A Thirty-Year Perspective on Competition and Consumer Protection* (Oxford University Press, 2013), pp. 83-108.

uncertain. Citing these uncertainties, the FDA threatened to seize All Bran as an unapproved new drug. When the FTC and the NCI defended Kellogg, the FDA changed course.

An FTC Staff Report documented the impact of the Kellogg campaign and its aftermath.[8] Increased advertising about fiber content and its relationship to cancer risks led to significant changes in cereals.[9] Claims about the relationship between diet and disease increased elsewhere as well, with similar marketplace impacts. For example, claims about the relationship between diet and heart disease rose from less than 2 percent of food advertising in 1984 to more than 8 percent in 1989;[10] consumption of fat and saturated fat, the primary dietary risk factors for heart disease, fell far more sharply after 1985.[11] Again, advertising led to beneficial changes in diet.

Advertising is particularly important to less advantaged groups. The FTC Staff Report documented that although fiber consumption increased for all groups, it increased more among racial minorities and single parent households.[12] Another study has shown that the least educated paid the highest increase in prices when eyeglass advertising was restricted. [13]

Online advertising can be expected to have similar effects to any other advertising, and those effects are generally good for consumers. Restrictions that impair its effectiveness can only reduce those benefits.

---

[8] Pauline Ippolito & Alan Mathios, Health Claims in Advertising and Labeling: A Study of the Cereal Market, FTC Staff Report (1989), *available at* http://www.ftc.gov/be/econrpt/232187.pdf.

[9] For example, the fiber content of new cereals increased 52 percent, and the weighted average content of cereals (reflecting both product changes and changes in consumer choices) increased at a significantly higher rate than before health claim advertising began. Ippolito and Mathios, *supra* note 8.

[10] Pauline Ippolito & Janice Pappalardo, Advertising Nutrition & Health: Evidence from Food Advertising, 1977–1997, FTC Staff Report (2002), *available at* http://www.ftc.gov/opa/2002/10/advertisingfinal.pdf.

[11] Pauline Ippolito & Alan Mathios, Information and Advertising Policy: A Study of Fat and Cholesterol Consumption in the United States, 1977–1990, FTC Staff Report (1996), available at http://www.ftc.gov/be/consumerbehavior/docs/reports/IppolitoMathios96_fat_long.pdf.

[12] Ippolito and Mathios, *supra* note 8.

[13] Lee Benham & Alexandra Benham, Regulating through the Professions: A Perspective on Information Control, 18 J.L. & Econ. 421 (1975).

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

Mr. LATTA. Well, Dr. Beales, thank you very much for your testimony today and, again, I want to thank all of our witnesses for being here and we'll move into the question and answer portion of our hearing.

I will begin the questioning and recognize myself for 5 minutes.

Ms. Glasser, would you describe some of the tools that are used to track consumers online and would you also tell what kinds of information digital ad businesses have about consumers and what they use it for?

Put that mic on, please. Thank you.

Ms. GLASSER. Thank you. Thank you, Congressman, for your question.

Sure, there are many different tools that you can use to track users online. I think it really could depend on the platform that you're using.

Persistent identifiers tend to be of the most common and those would include things like cookies or advertising IDs. They don't identify an individual personally so they're not personally identifiable. Instead, it allows to—it allows the advertiser to make associations and inferences on the types of behavior and the types of things that a consumer enjoys.

And can you repeat the second part of your question?

Mr. LATTA. Yes, and would you tell us also what kind of information the digital ad businesses have about consumers and how it's being used?

Ms. GLASSER. Sure. Again, I think that also depends on who you're speaking to in the supply chain. But, generally, for a company like mine, the type of information that we usually hold on the consumers would be things related to a cookie.

So that could include an IP address, cookie ID, browser information. For example, if you're using a certain version of Google Chrome or Internet Explorer, it might include a time stamp and a date for verification purposes. It could really vary, depending on how you set the cookie to collect information.

Mr. LATTA. Thank you.

Mr. Zaneis, how significant of a problem are bots and fake accounts in the digital ad ecosystem?

Mr. ZANEIS. There's no question that it's a massive challenge and a problem for the entire ecosystem. I think then there's a recognition that no industry can be based off of this high level of fraud.

The number that you quoted of 22 percent fraud in certain display units—you know, we used to have a discussion around is fraud 20 percent of all inventory or 30 or 40 percent.

Over the last 2 years, we've sort of turned the corner on that. We have not solved it. But now what we see, again, working with reputable partners it's relatively easy to get your fraud rate down well into, as I mentioned, less than 1.5 percent.

I sometimes look at other industries like, you know, produce shippers and manufacturers that have spoilage and breakage rates around 15 to 20 percent and I look at where we are getting the industry and think we are doing a good job.

Mr. LATTA. Let me follow up on that. Is there a conflict of interest in the industry if fake accounts are driving traffic numbers higher?

Mr. ZANEIS. No. I think that that's a common myth that has been put out there by some advertising naysayer—that because there can be more revenue generated by more traffic, even fraudulent traffic.

There's no question that some companies—legitimate companies—could make more money from that. We always say in the industry that there are crimes of omission and there are crimes of commission, and sort of sitting back and maybe getting a little extra revenue from a few fake hits on your website used to happen all the time.

Nobody in our industry is committing commission crimes of actually committing fraud, but I am happy to say that now the respectable companies—as I mentioned, 680 companies have sought to join TAG—now we've turned the corner on the crimes of omission.

Mr. LATTA. OK. Thank you.

Ms. Glasser, in about my last minute that I have, if I wanted to create a website today and sell advertising space, for example, a banner ad, and some ads along the side, how difficult would that be and how much would it cost me to get started, especially if I was a small business?

Ms. GLASSER. I would not be able to comment on what it could cost or even a range, because that could really depend on the size of the audience you're trying to market to or that you're trying to attract to your website.

It could also depend on the type of the audience, right?

Mr. LATTA. How about the difficulty, though? How difficult would it be for somebody to go out there to do that—to get a banner?

Ms. GLASSER. It's not very difficult. You would most likely have to engage with either—I think the easiest thing to do would be engage with an ad agency because they could basically do everything turnkey for you, or you could probably approach some ad networks on your own.

I've really only worked with ad networks from an agency perspective so I wouldn't know how it is personally to go and do it. But I think some of the bigger companies and some of the companies who have been around a lot longer probably, you know, have certain teams to handle the smaller businesses.

Mr. LATTA. OK. Well, thank you. My time has expired and I will recognize the gentlelady from Illinois, the ranking member of the subcommittee, for 5 minutes.

Ms. SCHAKOWSKY. Thank you.

Mr. Brookman, in your written testimony you say just last week, Vice published a story purporting to prove that Facebook listens to ambient conversation for the—for ad targeting purposes.

You acknowledge that privacy researchers cast doubt on the story but the fact that leading authorities cannot even agree on whether Facebook is mining personal audio conversations is emblematic of the generalized confusion about privacy.

We do know, for example, that Samsung's smart TVs do record everything. They have some sound—some voice-responsive feature. And I don't know what disclosure means, if it's in, you know, some sort of tiny print thing that you can find when you unbox the TV.

We also know that Vizio, also a TV, tracks second by second viewing information. There is right now an FTC enforcement action, or there was, against them because they did not disclose that.

So, you know, what do consumers know and what don't they know and how should they know, and should this be done even if they are informed?

Mr. BROOKMAN. Yes. No, I think that's a good question.

You know, I think there's just a lot of understandable uncertainty because there's so many sensors, right, all around our house.

We have Echos. We have—we have a microphone right now. I mean, according to that Vice article, you know, any company could be listening to it.

I do think that, you know, there are actually—some companies are kind of scared to go there. I know that Samsung in their privacy policy reserved the right to listen to everything you do. But they did, I think, fortunately, clarify that no, we will only actually listen when the button is pressed down, and I think that's the right choice.

Facebook has also tried to clarify, you know, we will only, you know, listen, you know, if you—we don't listen to what's going on ambiently.

But I think that's the question. I mean, according to Dr. Beales' testimony, it would actually probably be good if Facebook were listening to every single thing that I say and not just Facebook but also Google or Samsung or any of the 650 companies that Mr. Zaneis mentioned because it could give us, you know, more targeted ads.

I think consumers reject that and I do think it's actually unfair to kind of try to put that burden on consumers to try to figure out, you know, what every single company is doing, which is why I definitely support what you're saying—that there should be some basic rules of the road to empower consumers to kind of take some control over all these devices.

Ms. SCHAKOWSKY. Thank you.

What do you mean by rules of the road? Should we be passing legislation?

Mr. BROOKMAN. Yes. So there's a few things that could be done, like just better transparency for first, right? I mean, right now privacy policies—if you—if you look at them—you know, I review privacy policies as part of my job. I can't make heads or tails of them, and that's my job, right? They don't actually say what companies are doing. They reserve really broad rights to do stuff.

Actually requiring disclosure kind of like SEC filings would, I think, will probably have some degree of accountability for consumers who should not be affected, read those but for regulators and for folks like me who, like, try to rate products based on these sorts of things, there should be easier kind of global choices. I talked about do not track, which is a thing that I worked on for a long time. You should be able to, you know, opt out of everything at once. I mean, maybe it should be opt in for some things, right, or maybe some things that just shouldn't be happening.

You know, principles like data minimization—don't just collect every single thing, like, through the microphone just because it

might be interesting one day. You know, security—well, we don't have baseline security legislation in this country.

The FTC has done a pretty good job of trying to interpret the statutes to require it. But they've run into some roadblocks. You know, access to your information—if the company has the information about you they should tell you about it.

And so, I mean, there's been proposals floating around I think there are some good elements to, there's some bad element too, but, certainly, where we are right now where there's very little law, right, the basic privacy law is Section 5 of the FTC Act, which just says don't lie. And don't lie is a good principle but it's not enough, right? I mean, don't lie — if it's why I have these privacy policies I can't figure out what they're saying.

Ms. SCHAKOWSKY. In the few seconds I have, how common is it that there's discrimination in terms of—and maybe that's a loaded word—but in terms of hiring ads that do, particularly, age discrimination?

Mr. BROOKMAN. Yes. So I am familiar with the ProPublica work that was pointed out—you know, targeted ads for age but also, you know, you are allowed to target ads based on racist terms, right?

And part of the problem is, you know, Facebook is, like, a $500 billion company, or whatever—they make a lot of money—but they don't have a lot of staff, right?

They don't review all these things. It's all automated. It's all programmatic, which is efficient in some ways, but it's harder to snake out the fraud and the discrimination.

And I have a lot of respect for the work that Mr. Zaneis does to try to tackle that. But by and large, I mean, you look at the sort of ads that you see online. A lot of times they're a bad experience for consumers.

Ms. SCHAKOWSKY. Thank you. I yield back.

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

The Chair now recognizes the gentleman from Illinois, the vice chair of the subcommittee, for 5 minutes.

Mr. KINZINGER. Well, thank you, Mr. Chairman. I thank you all for being here today.

Professor Beales, we want the internet to continue to thrive but we also don't want consumers to lose faith in the internet because their information is being used in an unanticipated or even a harmful way.

Aren't there some baseline protections that would balance both innovation and consumers' trust in the privacy of their sensitive online information?

Dr. BEALES. Well, I think the approach you're trying to get consumers to understand the gory details of how this works and make choices on a provider by provider basis is just hopeless.

It's like trying to understand—trying to ask consumers to understand all of the code that's on your computer and how it works and what it does. It's not going to happen.

It shouldn't be used—the information, however it's collected and by whoever it's collected, should not be used in ways that are harmful to consumers.

But you need to figure out what harm you're worried about and figure out what's the best way to stop that harm specifically. It's

not an information problem. It's what people are doing with the information and if there's specific things that they're doing that are bad that's what you ought to address.

But targeted advertising isn't one of those.

Mr. KINZINGER. Yes, and so that you basically answered my second question, which is shouldn't the privacy protections be based on the potential for consumer harm and I think ——

Dr. BEALES. Absolutely. Absolutely.

I mean, I think it's always been telling to me that in Europe it's about data protection and in the U.S. we do privacy through a consumer protection agency.

Mr. KINZINGER. More people now access the internet from a device—phone, tablet, or IOT product—than from desktops or laptops. Knowing the geolocation of a consumer is increasingly important to these companies. Not only can companies target ads based on location but companies like Google and Facebook can assemble profiles and patterns of life about consumers.

I would like to hear your opinions about as to whether precise geolocating information should be considered sensitive information, meaning consumers should have to affirmatively opt in for tracking and collection of their location.

So Mr. Zaneis, can you explain to me how consumers are tracked between devices and how is it that ads on one device might be seen on another?

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

Just to be clear, TAG does not work on consumer privacy issues. But I certainly have a lot of experience here and have testified in front of the subcommittee in the past on privacy issues and data issues. So I am happy to elaborate a little bit.

Certainly, there are technologies—desktop and mobile browsing is technologically different than mobile apps, and cookies don't generally exist in the mobile app space. So you have different types of identifiers such as device identifiers for a mobile phone or a tablet that can be used.

But the concept is the same, which is advertising requires an identifier. Whatever it is is less important. The technology that empowers it is less important than what it is, and we've proven, as an industry—Ms. Glasser mentioned the Digital Advertising Alliance and the Network Advertising Initiative to wonderful self-regulatory programs not dissimilar from TAG that have been able to put in place consumer protections even in the mobile space.

Really, the key is to be technology agnostic but to set policy and self-regulatory principles based on principles and standards that everybody must meet. I think that's the effective method.

Mr. KINZINGER. Thank you.

Back to you, Professor. There's been a lot of debate about the concept of selling data, which culminated with the Facebook hearings recently.

These large online businesses often assert that they don't sell their consumers' private—personal information to anyone. Yet, five data companies—Google, Facebook, Apple, Microsoft, and Amazon—represent a combined market share of nearly $4 trillion.

So regardless of ownership of the data, they're well compensated for their commodities through the transactions that they conduct.

What do you think of their claim that they don't sell consumer data and is it really as nuanced as they—as they say?

Dr. BEALES. Well, the way I've seen it in the context of ad exchanges for—you know, for the purchase and sale of the advertising is there's not data that's bought and sold but there are cooperators in that process who are sharing data.

For example, an ad comes up that General Motors might be interested in. The publisher sends some information about what it knows about me based on the cookies that are on my machine to the ad exchange.

Somebody who's a potential bidder, like General Motors, who knows something else about me matches that information and now they know more than either party knew in the first place and they use that information in deciding on whether to bid on the ad.

But people think—companies in this space tend to think their data is their lifeblood and they're not going to give it to somebody else. I mean, they hold on to it as closely as they can is the experience I've seen.

Mr. KINZINGER. And just—with 10 seconds, because I am going to just get yes or no—consumer privacy laws and policy makers have regularly complained about the length and complexity of consumers facing privacy policies.

Do any of you believe consumers have a clear understanding of what's contained in a privacy policy? And so a quick yes or no from each of you would be great.

Ms. GLASSER. No.

Dr. BEALES. No.

Mr. BROOKMAN. No.

Mr. ZANEIS. No.

Mr. KINZINGER. Thanks. I yield back.

Mr. LATTA. The gentleman yields back and the Chair now recognizes the gentlelady from California for 5 minutes.

Ms. MATSUI. Thank you, Mr. Chairman, and thank you very much for our witnesses here today.

As we discuss here today and in previous hearings a fundamental tenet of digital advertising is explaining to consumers what data is being collected and for what purpose—in other words, providing meaningful and robust transparency.

But that, of course, is more complex than a list of the information on the types of data collected and whether that data is sold.

Specifically, companies are able to take user data and sell ads based on the data users provide to those platforms without having to ever sell that data to a third party, and the more data that platforms have access to and, importantly, the more they can use that data to create inferences to target these users, the better these platforms can target advertisements.

Entire panel—so even if data isn't so-called sold, how do we work towards meaningful transparency with both more clarity and nuance about data usage that don't make distinctions without differences?

Anyone want to start?

Ms. GLASSER. Sure. I think, plain and simple, we just need to be better at describing what we do. It is a complicated space. It does get very technical and I think the easiest way to explain what we

do is to provide an example. Explain to the user what happens when they go to Facebook or why they're seeing a certain ad.

I think in addition to that, the self-regulatory groups have made a tremendous effort toward that end by creating an icon that's supposed to indicate when certain types of advertising is happening or a certain type of data collection is happening for interest-based advertising which I talked about earlier.

Ms. MATSUI. Right.

Ms. GLASSER. I think we just need to be more clear and we need to write these policies much better.

Ms. MATSUI. Do you agree?

Mr. ZANEIS. I do. I mean, we all just agreed that privacy policies are not understandable by consumers just because you have to tell the truth but that's all you have to say and you have to disclose everything. It's not a—it's not an effective mechanism for disclosure, which is why programs such as industry self-regulatory ones—the DAA and NAI—are so important.

A lot of these third-party entities don't have a consumer touch point. So having a very simple policy disclosure outside of a privacy policy is key, and I will just add I think then the platforms that do have a consumer touch point have done a fantastic job of developing things like privacy centers and communicating with their users clearly.

Ms. MATSUI. OK. OK.

Mr. BROOKMAN. Yes. I mean, I think you're right that companies like Facebook or AT&T they make a big deal of the fact that they don't sell the data, right, but then it goes down to the question of excess data collection.

You know, I give Facebook a lot of information about me on plenty of stuff—pictures of my kids, things I like, my religious and political affiliation.

But that's not good enough, right? I mean, they actually—and this was I thought a fascinating part of the Cambridge Analytica hearings—a lot of the questions were not about Cambridge but how Facebook watches what I do in all my other apps and websites, and that's the thing I think a lot of folks object to.

So, really, you know, AT&T is like a service provider for me. They never used to listen to my phone calls to try to target ads to me. Do they have a—should they be able to watch everything I do online where I have no control because they're my pipe in order to target ads.

I think that's the sort of out of context data collection and use that I think consumers object to. I think they're surprised by that. I think that there should be maybe more prohibitions but very much at least some sort of rights.

Ms. MATSUI. Do you think the public is more aware of this today based upon what's happening—the coverage?

Mr. BROOKMAN. I think—I think there's a generalized awareness that our privacy is under siege. This kind of goes to the questions from Ranking Member Schakowsky. I think people feel like, I am being listened to all the time by everyone—what do I do about it—what's happening now. And I think there's just a lot of paralysis and a lot of confusion and a lot of, like, upset, right? I mean, we

talked about the poll numbers. People don't like it but they don't know how to——

Ms. MATSUI. They don't know what to do.

Mr. BROOKMAN. They don't know what to do. That's exactly right.

Ms. MATSUI. OK. How about you?

Dr. BEALES. Well, as I said, I think—I think the key is to think about what it is that we are worried about would happen as a result of this information and then think about ways we can keep that from happening.

The information is out there. It can be observed in a lot of different ways using a lot of different technologies, and new ones will be invented if not every day every year.

Ms. MATSUI. Right. The horse has left the barn, to a degree, so we have to figure out what we could do about it and try to explain it to everybody so people understand it, and then it's more of sense of how we deal with our own data and understanding as we click on things what could happen, right?

Yes. OK. Well, I am running out of time so I yield back. Thanks.

Mr. LATTA. Thank you. The gentlelady yields back the balance of her time.

The Chair now recognizes the gentleman from Michigan, the chairman of the Subcommittee on Energy and the former chair of the full committee, for 5 minutes.

Mr. UPTON. Well, thank you, Mr. Chairman.

Ms. Glasser, I want to follow up a little bit on what Ms. Matsui said. In your testimony, you stated, quote, "Using and sharing a consumer's name or similarly identifiable information is not necessary in many cases to provide rich, personalized, and relevant advertising."

So what's your thoughts as to why Facebook does in fact collect so much information along those lines like phone numbers and location and calling histories? What information—what are they doing with that if they don't really need it and to tee up that interest-based ad?

Ms. GLASSER. Thank you for your question.

Mr. UPTON. If you want to comment. I don't——

Ms. GLASSER. Yes. I can't speak specifically to the motives behind Facebook for doing it. Just simply, I don't have that insight.

However, my perception of the reason why they collect it is when you sign up for their platform, you have to provide this information so you can create your actual profile page.

Now, as I understand it, I don't think you actually have to give your phone number but in that case if you decide to it's a way that they can—they use it for a means to text you certain sort of updates or they can use your phone number to identify that particular device and be able to provide you continuity of services. Maybe you get a new phone but, you know, the phone number is the same. The device is different. It's a way for them to keep linking it.

Facebook is sort of a unique case in the broader ecosystem because they are a subscription-based platform. When you go to Facebook you provide your email, your name, and all of that information as a condition of signing up.

I think when you are looking on a website just like New York Times, for example, or the Washington Post, unless you have a subscription—let's assume you don't—you're not providing any of that information.

You're not giving your name, your phone number, your email address, and you don't need to in order to get advertising placed on that site that's relevant to your interests or things that you might have looked at before.

Mr. UPTON. So you mentioned a little bit earlier about the icons and I know that the Digital Advertising Alliance launched last month an industrywide initiative including a political ad icon for consumers.

Are you aware of any political ads currently branded with that new icon?

Ms. GLASSER. I don't, but I just haven't seen them myself. I am sure I will start seeing them after this conversation because it always comes up after you talk about it. But I have not myself seen them yet.

Mr. UPTON. Great.

Mr. Zaneis, can you explain how the third-party validation processes exist and how they work?

Mr. ZANEIS. Third-party validation as far as our certifications are concerned? Thanks for asking the question.

You know, any certification program is only as strong as the validation process behind it. So we work with a number of independent audit firms and the majority of our members actually go through a third-party audit, which is very significant and they literally are on the site, kicking the tires, looking under the hood to make sure that the companies are complying with our standards, and I will take it one step further, because if you go up the supply chain a little bit a lot of our efforts to fight criminal activity are supported by really niche technically sophisticated companies—what we call vendor companies—an anti-fraud vendor, for example—which they also go through an independent accreditation from the Media Ratings Council. So they may go with EY or somebody like that and go through a very extensive certification process.

It's really key to raise the bar.

Mr. UPTON. Well, I just want to say as a native Michigander I really appreciate your testimony. Thank you.

Mr. ZANEIS. I appreciate it. Thank you.

Mr. LATTA. The gentleman yields back and the Chair now recognizes the gentlelady—oh, I am sorry, I think Mr. Green just walked in.

Mr. Green is recognized for 5 minutes.

Mr. GREEN. I want to thank the chairman and the ranking member for holding this hearing. The two biggest online privacy scandals in the past year has come through this subcommittee—the Equifax breach and the Facebook Cambridge Analytica issue—and I hope we can soon see some legislation on the books to protect Americans online.

Mr. Brookman, we know that small businesses as well as larger corporations sometimes benefit from consumer data since it allows them to show their ads to customers who are mostly likely to want their product.

Do you know—do we know how common it is for small to medium-sized businesses to use tracking technology as compared to larger businesses?

Mr. BROOKMAN. I don't have that information. But I will grant the point—that it's small businesses, large businesses. Lots of companies rely—use behavioral targeting ad tracking to reach their customers.

I will also concede Dr. Beales' point that in some cases those ads may be more valuable. I do think the vast majority of ads are not in fact behavioral and I do know that leading publisher trade associations like Digital Content Next—they used to be the Online Publishers Alliance—have been one of the more aggressive forces calling for actually privacy protection. Even though—and we are a member too, right?—I mean, even though those companies use targeting, they think it would be better for the ad ecosystem if there were some more protections in place.

It would be partly just for confidence in the ecosystem, partly because a lot of the excess consumer surplus is just flowing to companies, to Facebook, and to Google and also because, I mean, they're seeing companies or users deploy ad blockers because the self-regulatory efforts that have happened so far haven't been sufficient to address a lot of these concerns.

Mr. GREEN. OK. Any—do you have any thoughts on whether there are any way for any potential online privacy law at the Federal level to balance potential benefits to businesses along with better consumer privacy?

Mr. BROOKMAN. Yes, absolutely.

I mean, it's a thing that I've worked on for a number of years. The United States is kind of an outlier around the world and most countries have some sort of basic privacy laws on the books to give folks control.

United States is one of the rare exceptions so they don't. The default law is just don't lie to folks, which has not been sufficient to really safeguard privacy.

So yes, having something on the books that provides better information—again, I don't want all the onus to be on consumers to try to figure out, you know, every single thing so I think, you know, a lot of this out of context data collection, data usage, may be, you know, should be prohibited in some cases, right?

At the very least, though, there should be some more—at least a stronger ability to say no, right? A lot of folks just—you know, they feel like they want control. They feel like they're being monitored. They wish they could do more. They don't have the information or ability to do so today.

Mr. GREEN. Well, and after our hearing with Facebook, we realized that, you know, somewhere along the way you can't accumulate this data without marketing it and that's the reason.

But like you said—and I hear, you know, the balance of the consumer privacy—I really want to get permission for it. I don't want them taking it from me without knowing.

Can you discuss ways to balance the consumer privacy, which polling shows is extremely the high priority for Americans, with any benefit that may sometime come from these ads?

Mr. BROOKMAN. Yes. I mean, Facebook has a lot of information about me. They have—like, they know where I live. They can serve me plenty of targeted ads.

What I object to is them watching every place I go online, you know, in order to monitor me in ways I don't expect.

They started doing that back in 2011 or so when they started rolling out like buttons and people would see a like button—"Oh, I can press this, I can click 'like.'"

What it didn't realize is that meant Facebook was watching them whether they clicked the button or not, right? And so that's the sort of thing I think folks object to. That's the sort of thing I think—I saw a lot of Members of Congress were objecting to during the Cambridge Analytica hearings—that's the sort of thing I think consumers, like, don't expect and that there should be stronger rules in place for, whereas today there really aren't.

Mr. GREEN. Well, I even have a staff member who said he was planning to get married so he was looking for wedding rings, and all of a sudden he saw these adds all pop up on his handheld.

So, I mean, it's a problem but how do we deal with it? While you were at the FTC you worked on a commissions cross-device tracking report. Can you tell us some of your concerns about companies following people across these multiple platforms?

Mr. BROOKMAN. Yes, absolutely. So I think it's just unexpected in ways that folks, you know, don't necessarily think that just because I am on my phone I will suddenly—if I am searching for "wedding ring" on my phone, suddenly on my desktop computer—which, by the way, I share with my live-in girlfriend—suddenly she starts seeing pop-up ads over there for the wedding rings I was looking at.

I think a lot of folks don't necessarily expect that, and I think they——

Ms. SCHAKOWSKY. You better get married.

[Laughter.]

Mr. BROOKMAN. Exactly. It's a lot of pressure.

But I think, I mean, the information is used in ways that are surprising. So online tracking used to be fairly anonymous, but now if you go a publisher you type in—if you log in on, you know, Justin at Gmail, you know, that website might then spew out to a bunch of ad networks, hey, that's Justin, right? And so they are now tracking by real name in ways that they hadn't done before.

And so I think these are the sorts of things that are unexpected, and I think when people know about them, they're up in arms. They're controversial, and they wish there were more limitations or at least controls around.

Mr. GREEN. Mr. Chairman, just briefly, I heard that if I have a smart TV and I have my handheld, my iPhone, they can actually know what they're doing and together. Is there any solution there? Should we just turn it off?

Mr. BROOKMAN. Yes, it's tricky.

Mr. GREEN. I really don't like the appliances talking about me.

[Laughter.]

Mr. BROOKMAN. It's a big conspiracy, and I wish they would knock it off.

You know, things like—most of these companies do offer, like, opt out. So there are controls, but they're kind of hard to find.

And so, I mean, one thing we try to do in Consumer Reports is, like, say, "Hey, if you want to knock this off, here's how to do it."

It's just, like, a lot of labor, right? I mean, we all have a lot going on. We don't want to have to spend, like, half an hour configuring our smart TV to, like, not talk to the toaster, right?

I mean, there should be some things that by default just don't happen.

Mr. GREEN. Thank you, Mr. Chairman.

Mr. LATTA. The gentleman's time has expired and yields back, and the Chair now recognizes the gentleman from New Jersey for 5 minutes.

Mr. LANCE. Thank you, Mr. Chairman.

I want the panel to know I've been happily married for a generation, and none of these matters pop up on my computer.

This subcommittee had Mr. Zuckerberg testify before us two months ago. As others on the panel have indicated, reports last week revealed that Facebook has data assuring partnerships with many device makers, including Chinese firms that U.S. intelligence agencies have labeled national security threats.

Following these reports, I sent Mr. Zuckerberg a letter indicating my continued frustration with Facebook's handling of users' data.

I reiterated a statement I made at our April hearing that I believe Facebook may have violated its 2011 consent agreement with the Federal Trade Commission.

I believe Facebook's issues are interrelated with the subject of this hearing, digital advertising, as the company makes the vast majority of its profits from advertising, reporting $40 billion in revenue from advertising alone in 2017.

Another issue I am concerned about is the increase in fake news advertisements and foreign interference in our electoral process.

I am one of the co-sponsors of the bipartisan Honest Ads Act, which enhances disclosure requirements and transparency for online political advertisements.

I was pleased that Facebook pledged its support to the bill, and I thank the panel for being with us this morning.

To the panel in general: From your expertise, how do companies balance the need to protect privacy while also offering the most effective advertising platforms to their clients?

Ms. Glasser.

Ms. GLASSER. Thank you. There are a lot of things that we do before we engage with a company for advertising or analytic services.

To us, it's of paramount importance to make sure that we are working with companies who behave appropriately and who do the right thing. It's our reputation on the line, and if we get caught up in things like misuse of data or data collecting—being collected improperly, you know, that's a clear black mark on us.

At the same time, we can't obviously control other companies. However, we have some expensive due diligence that we put in place, whether it starts with reading a company's privacy policy, ensuring they offer opt-out, ensuring they're actually describing how their services work, if they just describe data collection on

their own website that doesn't necessarily get us where we need to be because consumers are using their services and their platforms and not necessarily their website.

So we go through some extensive efforts to make sure that the companies we are working with are at least taking an effort to do the right thing, whether it's members of industry associations such as TAG or the NAI and DAA, it provides a level of comfort to know that they too recognize a lot of the issues and that they too are obliged to put certain protections in place.

Mr. LANCE. Thank you. Others on the panel?

Mr. ZANEIS. Yes. I think Ms. Glasser nailed it as far as every company really has to take privacy very seriously because it impacts their reputation in his market and it's a very fluid market. It's a very diverse market, and consumers can go to any of your competitors with one click.

In my experience, it's been companies—early adopters in self-regulatory programs—it's a good signal that they care about it and in working it helps establish both the Digital Advertising Alliance almost a decade ago and now TAG 3 years ago. Facebook has always been an early adopter and a good participant.

Mr. LANCE. Mr. Brookman.

Mr. BROOKMAN. Yes. I mean, I will ultimately grant that, you know, I have friends that—who work at privacy companies and they do a lot.

I just think that the balance is off—that there's always this wide-eyed enthusiasm that big data will save everything while folks tend to be very dismissive that things might go wrong.

And I think, you know, the consequences if they go wrong, there really isn't enough risk. There's not any—Ranking Member Schakowsky talked about how the Federal Trade Commission—you know, even if a company does violate the fairly week laws that we have can't get penalties in most of the cases. They have a limited staff to police—like, again, all these things that, again, leading academic experts can't even figure out.

When I was at the FTC, you know, I worked in their division, their office of technology, research, and investigations designed to try to help bring more tech expertise to the FTC. But we were understaffed. And so I think, you know, there's just not enough reason to try to safeguard privacy in the existing legal framework.

Mr. LANCE. Thank you. My time has expired but I look forward to working with all of the distinguished panel members.

Thank you very much, Mr. Chairman.

Mr. LATTA. Thank you. The gentleman's time has expired, and the Chair now recognizes the gentlelady from Michigan for 5 minutes.

Mrs. DINGELL. Thank you, Mr. Chairman.

I am not calm like anybody here. I listened to all of you this morning. I've listened to my colleague, Ms. Schakowsky. I don't have an Alexa in my house. I don't want anybody listening.

We've seen examples of people knowing that we are being listened to and, you know, in the past we've been told to just trust companies that hold our personal information, and that our information was used in a transparent process.

We, obviously, now know that that's not the case and I think, quite frankly, the trust is wearing thing. You say, well, consumers are kind of worried about it but what can you do about it.

Consumers don't understand how much that data is being used and how it can be used.

Dr. Beales, I didn't sleep last night. I was up all night for two reasons. One, I pulled out my paper from my graduate school on public good, and I think that what we are talking about today in the internet is not a public good and I am going to write a paper.

I was up until 3:00 a.m., and you're going to be the first copy to get a—first person to get a copy of it.

And two, Michael Chertoff has a new book out on privacy and was talking about how the Chinese are using all of this data to actually—we think it's innocent.

The Chinese are looking at who does these searches and compiling them and grading them, and how people get jobs, et cetera, and that's what's happening here.

How do we know that this data, viewed alone, thousands of data points collected on each of us, don't paint a picture other than our, you know, our interests, curiosities, or preferences?

But when they're combined together, they create a vivid mosaic of both our online and offline who we are, and we don't know who that's being shared with, and trust me, I don't trust you to say it's not being shared with lots of people.

It should raise concerns for consumers. We've got laws that protect people at work, on the streets, and in their homes, and with the lines continually blurring between online and offline.

I think we have to address these issues and we need to be doing a lot more to protect consumers and educate them. They think there's nothing they can do and what does it matter—it could matter a lot.

So, Dr. Beales and Ms. Glasser, what are the market incentives for companies to not collect as much information as possible? There are none, I would like to say that.

Dr. BEALES. I think—I mean, collecting information has some cost. It's usually not very big, and so the incentive tends to be to collect more of it, and we'll see whether it is good for something.

There's an incentive not to collect, I think, information—that people are going to be reluctant to give you. I mean, if you do survey research you always ask questions about income at the end because a lot of people will stop answering question when you ask that question and you don't want to lose the data. There's not a lot of incentive.

Ms. Glasser.

Ms. GLASSER. Sure. I think that there is definitely a lot of—a lot of reasons why companies would want to limit the data that they're collecting, first of all, for legal reasons, right? I mean it depends on which sector you're in and, as we all know, there are different sectoral logs here in the U.S. that protect different types of information, particularly CAPA.

Now, I don't want to collect personally identifiable information by children, which includes cookies and personal identifiers.

Same thing goes for health care or finance. I, as a company, have a vested interest to limit the data on collecting for several reasons.

I don't want to risk a lawsuit. I don't want to risk enforcement by the FTC, not even from a legal perspective—of course, that's terrible, but—I mean, depending on whose side you are, but also because I don't want the press and I don't want people to know that I got caught doing something I shouldn't have been doing.

I think the other reason is, if I am collecting all of this data that I don't necessarily need, I run the risk of collecting bad data, and when I am collecting bad data and it comes to be found out that it's bad data, then I have to go and purge all of my data that might be connected to that bad data and that comes at a tremendous cost to my company, literally, in money what it costs to have engineers and people go through the systems and do that. It also comes at a reputational cost as well and it could slow down business because we have to now remove this entire data set.

So for me and for our company, there's, clearly, a vested interest to collect only what's needed.

Mrs. DINGELL. So I am almost out of time. So I am going to do more questions for the record. But I will give you all another example.

I was prepping for a committee hearing. I stay up nights. They call me Dr. Google. But was doing opioid research and by the next morning was getting drug rehabilitation centers to check myself into, and I didn't want anybody to think that I was a drug user.

But that's the kind of data that's being collected and then a potential employer can buy that from somebody. People don't think about it. I hope we can get them to.

Thank you.

Mr. LATTA. The gentlelady's time has expired and the Chair now recognizes the gentleman from Kentucky for 5 minutes.

Mr. GUTHRIE. Thanks a lot, and thanks for being here. And this is serious and really trying to figure out where we draw the line in public policy in this.

I've said before that, you know, I am from Kentucky. I love college basketball. The most frustrating thing is every 4 minutes you get a TV timeout.

But I get to watch it for free because I got to watch the ad. And we are talking about free content. I think Mr. Brookman said people don't want to trade free content for the violation of privacy.

And what will be interesting in some of these apps would have a subscription so you can subscribe and you get no ads whatsoever and see what people choose. That would be interesting to see where people move forward with that.

But and I was in Ms. Schakowsky's district trying to figure out how to get around Monday—trying to get around traffic to get from Sheridan Road to Lake Shore Drive.

And the app I was using popped up an ad right when in needed to make a critical turn. So that was—so there's a difference in frustrating—but I was in your wonderful district. Might ever trying to get me lost so I would stay in Chicago.

Great city, by the way. And so we are trying to figure out what's, like, just nuisance and stuff you have to fool with and pop-ups and then really what gets into what some of the things that Mr. Brookman has talked about and where we need to draw a line.

So just kind of the process of this. So, Ms. Glasser, first, so how do the—these target audiences are created by additional ad companies.

I mean, just kind of how is that—I think we've kind of gotten into it. They look at all the different ways that you move forward. Can you kind of describe how a target audience from a digital ad company is created for—generically for somebody who's wanting to create an audience?

Ms. GLASSER. Sure, I would be happy to.

So, basically, what happens is we talk about intra space advertising. Typically, we'll used intra space advertising to build these profiles and target audiences and what we do then is we actually will see what websites you have gone to over the course of time.

So maybe one day you're visiting MapQuest to get directions. Another day you're on a gardening website. Then you're on the New York Times and then you're looking to buy dog food, and algorithmically and using modelling and science they are able to sort of piece these things together and, you know, put you in a certain age range—say, you're male, you live in Kentucky and you have an interest in gardening and dogs. Simple enough, right?

That's basically an interest category. We then provide that data to other partners for them to target the specific audiences but we'll use the data collected over different websites over time to build up these profiles and to get a sense of the different interests so that we can build these——

Mr. GUTHRIE. And then you build up ads that I want to see. That's the kind of the things instead of generic, like, when I do the basketball whatever comes on I got to watch but ads I want to see.

So I don't have an issue with that but just trying to figure out where we draw the line.

So, Professor Beales, you talk about or it's been suggested that online advertising market can operate like an financial exchange where people bid on the ads and people—I heard you talk about that earlier today.

How does that work? I mean, how does that kind of—I didn't realize that happened.

Dr. BEALES. Yes, there's an——

Mr. GUTHRIE. Usually, like here's a group of dog lovers from Kentucky so here's an ad that—and so somebody will bid on to get the ad——

Dr. BEALES. Well, you go to a website and the website will say here's an ad—here's the limited information that website has, other than you're on that website. That may be all it knows but it may be part of the network that knows something more.

It passes that information to the ad exchange, which passes it on to potential bidders, which are typically advertisers or advertising agencies who have other information about you.

Mr. GUTHRIE. Well, I will go to the—going to a website and boom, all this starts taking place instantaneously?

Dr. BEALES. Yes. Absolutely. Absolutely.

There's a fascinating video that I think is 70 milliseconds or something like that, which is about how long it takes to actually serve the ad.

Different advertisers bid. You know, I've got this great dog food that I know you're really going to like so I will bid a lot for your exposure. I win the auction, and the you get the dog food ad.

But there may be dozens and dozens of advertisers that bid for that particular availability, each of who has a little bit information about what—about you, about what you might be interested in, and the one who thinks you're most valuable is the one——

Mr. GUTHRIE. And, obviously, the more information I have the more valuable I become to that—whoever's bidding, obviously. The more they know my likes, the more they're going to bid on what I—and so therefore, to get me on somebody's website they're going to provide better content.

So I will use their—so they kind of—it works that way, but it just gets into the—but they have to have so much information on you so that—are there things that you think need to be protected in that or people just need to know, going in, and that it's an open process?

Dr. BEALES. Well, I think it's a more going in—a known going in and I think it's more think about——

Mr. GUTHRIE. The thing is if everybody's a good actor we are—I mean, the problem is the bad actor. If everybody's a good actor, then it makes me more valuable to that advertising.

It makes somebody want me on their website. They're going to provide better content that I will then enjoy using. That's why I go there. And so it all works. But how do you protect against the bad actors in that?

Dr. BEALES. I think you got to think about what I means to be a bad actor and then try to restrict that particular conduct. It's not that—it's not that a lot of people know something about you from your various online behavior.

It's what bad do we think might happen. I mean, Congresswoman Dingell's example of what China's doing—I mean, the problem there is the Government has got that data, and to the extent that that's a problem, that's a problem we can address directly by making it harder for the Government to get that data.

But it's what are—and I think we need to ask what are the bad actors doing with that information that could be harmful, because we need to try to address the bad things that could happen to consumers.

But it's not the information collection that itself is the bad thing. The bad thing is what somebody does with that.

Mr. GUTHRIE. OK. Thanks. I am out of time. I yield back.

Mr. LATTA. The gentleman's time has expired and the Chair now recognizes the gentleman from California for 5 minutes.

Mr. CÁRDENAS. Thank you, Mr. Chairman, also Ranking Member Schakowsky for having this hearing, and I would like to thank the panellists for answering our questions and helping us make sense of all of this, and there's a lot of all of this involved here. It's very, very new to the human psyche and the human element.

You know, this is on the heels of the Facebook scandal and the hearings that we've had here. But at the same time, I think that it's important to note that that's just the tip of the iceberg.

There's a lot going on out there and a lot that we don't hear about, and I think that Mrs. Dingell brought up some good points

about just getting online and all of a sudden the next day, you know, you get certain pop-ups and like she said, who knows in the future if people are going to use that against someone saying, hey, are you really an opioid addict because we got some information on you and you spent a heck of a lot of time looking at this stuff.

But then again, she's just doing research, but at the same time, people are going to use that data as they wish, and what is unfortunate is that we have a lot of small businesses out there who are benefiting from this, who are able to compete now in an environment like never before with larger businesses, that are creating jobs.

In my district alone, for example, it's come to my attention that thousands of jobs have been created just in my district alone because of this new technology and these new efforts.

And when it comes to the economic boon as well, there is economic pluses. When you talk about thousands of jobs, you're talking about hundreds of millions of dollars of money that's coming into my community.

So there is positive to all this as well. But where is the balance? And in that comes my first question is what data is collected from consumers and also what kind of data do companies pay for the most and what information about consumers is most valuable to them.

If anybody can give me some perspective on that.

Ms. GLASSER. I would be happy to try.

Mr. CÁRDENAS. Sure. Thank you.

Ms. GLASSER. I think the answer is really it depends. I think it depends on what your end goal is as far as what data will be most valuable.

I think it also depends on who you're trying to reach and what type of company you are. Again, I think all of us at least up here—I can't speak for everyone else—are true believers in data minimization, transparency, and principles along those lines.

So as far as data minimization you only collect what you need and that would not typically fall into the area of egregious practices.

Mr. CÁRDENAS. Anybody else?

Mr. ZANEIS. Yes, I would be happy to answer that, and it relates very well to Congressman Guthrie's question just a second ago.

Obviously, some of your web browsing behavior is going to be collected and so if you go to another website and we are talking about the real-time bidding, somebody then thinks since you want to buy dog food may think that you're worth, you know, 20 cents for that impression—somebody then knows that you just went to a—to autodealer.com or something like that—may think you're worth $20. And so that kind of information is very valuable.

But I also want to make sure we don't lose focus and get too myopic just on advertising because this kind of information is collected for all sorts of purposes.

At TAG, we collect from our member companies' IP addresses and we use them to fight fraud. We have something called a data center IP list and it has 40 million IP addressed that generate fraudulent nonhuman traffic.

This is incredibly valuable tool to fight criminal activity globally and it only comes from companies. So if companies are restricted from collecting that kind of information, perhaps under GDR-like restrictions or the California privacy initiative, that's going to harm law enforcement and industry's efforts to fight crime.

Mr. CÁRDENAS. Yes, go ahead.

Mr. BROOKMAN. Yes. So the question of, you know, what information is collected, I mean, I think my main thing would be that more and more information is collected from more and more devices in confusing and often in transparent ways.

So if I am with Congressman Guthrie watching a basketball game I think I am likely to expect some ads targeted to the content to what I am watching, right? I am going to see ads for trucks and for beer, and that's contextual and that's fine. I think people appreciate that.

What I might not expect is then for my ISP to then tie what I do on a connected computer, right, and maybe I am looking for wedding rings and suddenly I am watching the game and a big ad for wedding rings comes up based on what I did on a different device and watching the game with my girlfriend.

This is the thing I think people are confused by and it's increasingly capable, rights. I mean, TV ads used to be not targeted to individuals. Increasingly, they can do that, right, and tie it to your behavior online or they can tie it to the email address that you give them, and that's the sort of thing that I think people—we are all kind of grappling with.

You know, how do you put in place, you know, because it is valuable, right? I mean, yes, I suddenly need to spend a lot of money on the diamond ring right now.

But I think people still wish they had autonomy and control over the things they own.

Mr. CÁRDENAS. Thank you. My time has expired.

I yield back. Thank you, Mr. Chairman.

Mr. LATTA. I thank you very much. The gentleman's time has expired.

The Chair now recognizes the gentleman from Indiana for 5 minutes.

Mr. LOEBSACK. Thank you, Mr. Chairman.

I guess this could be one of those things, be careful what you wish for.

I remember 25, 30 years ago, you know, people thought this would be great. And it is. It really is. It's transformational to our world, but also there some downsides. It's a serious issue.

And Mr. Zaneis, you point out it's not only about ads, it's about national security. It's about all kinds of law enforcement. And so that's why we have to really strike a very good balance here about what we do regulatory-wise or legislatively as it relates to this issue.

I also think do you—does any—do we think that there's a generational difference in concern over this? Because I have some sons who are in their 20s and my son has an Alexa.

You know, I went to this apartment and he had it. I am, like, don't you—they just don't seem to be concerned about it. Do you think that's a problem? Do we need to—do we need more education

maybe of people who are now—have never grown up with the internet?

I mean, anyone—Mr. Zaneis—about why this is actually a legitimate serious question that it's just not about—just not about turning on some jazz music, which he did, which was really cool.

You see what I am saying?

Mr. ZANEIS. Absolutely, and I will say that there are—of course, there are generational differences. Without a doubt, folks that are, you know, digital natives and folks are not.

I will say this. Everybody cares about privacy, and sometimes you hear folks say, oh, young people don't care about privacy.

It's not that they don't care about privacy. It's that they understand the trade-off a little bit better in order to get services and they are more willing to trade off certain privacy and data in order to receive the services that they are sort of entrenched in.

So there are studies. I will just say that I am sure Mr. Brookman has some great numbers. Anybody can show you a study that says either 90 plus percent of people are really concerned about privacy or, you know, 90 percent of people love the digital services they get and are willing to trade off.

Mr. LOEBSACK. Sure. I understand.

Briefly, Mr. Brookman, because I've got several questions.

Mr. BROOKMAN. I think—I think young people actually do probably care about privacy just as much. They tend to be a little more tech savvy so they——

Mr. LOEBSACK. Do you think they're just resigned to the fact that it's not going to happen?

Mr. BROOKMAN. I actually don't because, like, for example, you think about who uses ad blockers, right? It tends to be millennials and younger people.

Mr. LOEBSACK. OK.

Mr. BROOKMAN. They have the ability—they feel they have more control to take back their privacy, I think.

Mr. LOEBSACK. This is a general question. You know, so I don't generally quote from the media but there was media person here in town that walked around town with a couple of smartphones.

One phone had all the things that was, like, on airplane mode, all the Wi-Fi and Bluetooth was off, and the other phone was hard turned off. I mean, it wasn't just—you know, they had it completely turned off.

Walked all around to different locations around DC—this is actually very fascinating—then went back to studio and then turned these phones back on, and had a tech person be able to monitor what happened once they turned them back on.

And all this meta data from everywhere they had been on both devices, by the way, even the one that was hard turned off, was—showed up on the screen and was jettisoned out to the world.

And so location—I think the location stuff is really important, because they had stopped at a park bench by the cathedral and went to a Starbuck's and all that, and all that was known.

Do we know—Consumer Reports would maybe answer this—do we know—was this a media—was this just the media that did it or do we know that phones do this?

Because it becomes a hardware issue, right? It's not a—this is a national security thing, because some of our—we have, you know, hardware that's been imported from all around the world that's in some of our devices, and our devices are made in other parts of the world.

I mean, do we know that this can happen?

Mr. BROOKMAN. So I've seen reports that Android phones, when location services are turned on, do collected a lot of information which I would personally find surprising—collect barometric information, seem to know what floor you're on and they guess whether you're on a train or on a bike or walking around—in ways that I think that a lot of people would object to.

I don't know that they do that when the phone is hard turned off. I think that would be bad, if that were the case, because it is an issue of security. Location information is very sensitive.

I get Google uses location for, like, really useful things like Maps, which I use all the time, right, and I believe they probably have some protections on the back end to anonymize it.

But, I mean, as a user, like, how do you know, and it is disturbing when you do find out the raw feed that does get uploaded, I don't know if it is quite as extensive as what you're talking about but it is extensive and surprising.

Mr. LOEBSACK. Yes. I mean, I just want to bring that point up that, you know, we are talking about apps and websites and everything. But for all the other reasons that Mr. Zaneis talked about other than advertising, we have to be concerned, I think, also about whether our hardware is that's in our devices and computers.

You know, we can turn everything—they turned everything off and it didn't matter. And whether that's true or not I don't know because it was a media report, but it's concerning.

I yield back.

Mr. LATTA. Thank you. The gentleman's time has expired and yields back.

The Chair now recognizes the gentlelady from California for 5 minutes.

Mrs. WALTERS. Thank you, Mr. Chairman.

Mr. Beales, this first question—it's a three-part question. It's actually for you.

What steps can be taken to enhance competition in the market for online advertising and what are some of the advantages and disadvantages of the way the market and the ad tech works today?

And are reports that Google and Facebook control 90 percent of the market true?

Dr. BEALES. Let me start at the end. I don't really know what the markets shares are, but I don't think 90 percent is remotely right.

I would think it's more like 50 or 60 percent. But that's a fairly well-establishable number that is not hard to find out.

And one of the interesting things about the online ecosystem is we don't know what's the most efficient way to organize this, and people are trying lots of different things and it's changing on a very regular basis.

I mean, the whole idea of ad exchanges is probably not 10 years old yet as a way to distribute this content, and people are finding

out the pros and cons of different approaches and then trying alternatives because it's a very innovative space and that is the engine of competition.

What got Google and Facebook to where they are was better mousetraps, if you will—different mousetraps in each case—and the competitive pressure in this market is in part from the third-party providers that don't have sign-in but do get some of the same information in indirect ways, and it's really important to preserve that competition.

Mrs. WALTERS. OK. Ms. Glasser, as someone who went to law school and studied privacy, do you believe that there's an adequate understanding or amount of training on data privacy by entrepreneurs, engineers, coders, and et cetera who build these products?

Ms. GLASSER. I can really only speak from some of my experience and what I've seen, and I don't think that there's enough education.

I am very fortunate where I kind of fell into privacy by accident where I was a law student at night working full time so I had to take what was available to me, and that was typically the privacy stuff because I guess no one else was interested in it.

But it turned out to be quite fruitful for me so I am grateful. I've always said that I am a firm believer in education and even if it's education about privacy or how to code or how computers work, I think education on how the internet literacy period is also extremely important, whether it comes to children, advertising, you know, how to help elderly people recognize scams or fraud.

Absolutely, I don't think—I don't think that we could do ourselves wrong if we encourage more education in this field.

Mrs. WALTERS. OK. Thank you, and I yield back the balance of my time.

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

The Chair now recognizes the gentleman from Florida for 5 minutes.

Mr. BILIRAKIS. Thank you, Mr. Chairman. I appreciate it.

Professor Beales, you mentioned in your testimony that advertising is particularly important to less advantaged groups, particularly minorities and single parent households.

I am also curious as to your perspective on the senior population. How would regulation in the advertising space affect these particular groups?

Dr. BEALES. Well, the—what the academic research shows about the impact of advertising is there are some people who are better at either using information or have more time to use information, and that's where those people who are good at information and have the time use information that's available from other sources and they're less dependent on advertising.

The people who don't have those advantages need the information in an easily digestible form and that's what advertising does is it boils it down to a very simple proposition of buy my serial, and I don't know where the elderly would fit on that.

On the one hand, they got a lot of market experience and that would tend to mean they're not going to be all that dependent, and on the other hand, they also have a lot of time in many cases and

can use other information sources in ways where they're less dependent on advertising.

I don't know of anybody that's looked at that question specifically.

Mr. BILIRAKIS. OK. Fair enough.

You talk about the importance of transparency in digital advertising. This question is for Ms. Glasser. You talk about the importance of digital—importance of transparency in digital advertising but suggest that a choice mechanism I snot always required.

Yet, one of the reasons we were holding this hearing is due to our constituents' concerns and the need to raise awareness about privacy.

Do you believe that the FTC has the tools it needs to effectively protect privacy and do you have suggestions for my constituents to prevent websites from collecting information about them?

Again, personal information—how do we protect personal information? And then, Mr. Guthrie mentioned that particular example but also Mrs. Dingell mentioned the example of the opioids.

Give me another example of a bad thing that can happen. I think our constituents need to know. So this question is for Ms. Glasser, please.

Ms. GLASSER. I think—that's correct. Not every instance requires and opt out. So what I meant by that, for example, if I own a website and I want to know how the behavior of users is on my website specifically, I want to know what features of my website users like to interact with.

I like to know what content they like to interact with, and this helps me build a better website. This helps me build a better platform for users to come to.

And I am not necessarily using this data for advertising or marketing purposes. It's really to help me understand the behavior of my business, essentially, and in those instances an opt-out is not always required.

However, I do think that transparency is absolutely key to all of this, whether you—whether you're using tracking pixels for analytics or you're using it for more engaged advertising and more engaged data collection.

I think it's absolutely critical that these things are explained to the end user and the consumer so that they do understand, OK, I see a tracking pixel on this website, but they're not using it for advertising—it's being used for analytics—I don't have to worry. Or if it's being used for advertising, I can expect to see the red shoes I am looking for show up on the next website I go to.

Only through our transparency can we even begin to expect consumers to understand what's happening.

Mr. BILIRAKIS. Again, link this back, for example, Mrs. Dingell's situation with the opioids, doing her research—and I commend her for it, doing the research late at night because I do it, too—and then maybe years down the road they might link her personal information to possibly being a drug addict or what you.

Is that the case? Can that happen?

Ms. GLASSER. I mean, anything is really possible, right?

Mr. BILIRAKIS. Yes.

Ms. GLASSER. It absolutely can happen. But I think it's also important to point out that within the industry—and we've talked a lot about responsible actors, legitimate companies, the self-regulatory groups—there are restrictions on using that type of information for targeting and behavioral advertising.

The NAI, for example, has very specific provisions on whether you can use health-related data—sensitive health-related data about sensitive categories—thing like drug abuse, drug addiction, mental health issues, cancer, sexually transmitted diseases, reproductive issues, all of those things are really off limits unless you have opt-in consent, which I don't know anybody who even actively goes after those types of segments just because of the sensitivity of it.

And I think when we put ourselves in our consumer shoes, none of us want to be targeted with those types of ads either.

So, again, I think it comes back to some of the points that Dr. Beales made and Mr. Brookman made about making sure that, you know, we hold the bad actors accountable and we continue to push these standards forward and we continue to try to enforce these standards so that we are using the right type of data to target the right type of advertising—the right type of people.

Mr. BUCSHON. All right. Very good.

Thank you, Mr. Chairman. Thanks for holding the hearing as well.

Mr. LATTA. Well, thank you very much. The gentleman's time has expired.

And seeing that there are no other Members here wishing to ask questions, I again want to thank our panel for being here today and presenting before us. Very, very informative.

But before we do conclude, I would like to include the following documents submitted for the record by unanimous consent: two documents from Oxford BioChronometrics, two documents from Interactive Advertising Bureau, a blog post from MPAA.[1]

And pursuant to committee rules, I remind Members that they have 10 business days to submit additional questions for the record. I ask that the witnesses submit their responses within 10 business days upon receipt of the questions.

And without objection, the subcommittee will stand adjourned.

Thank you very much.

[Whereupon, at 12:02 p.m., the committee was adjourned.]

[Material submitted for inclusion in the record follows:]

[1]The Interactive Advertising Bureau documents have been retained in committee files and also are available at *https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108413.*

Quantifying Online Advertising Fraud: Ad-Click Bots vs Humans

Adrian Neal, Sander Kouwenhoven
firstname.lastname@oxford-biochron.com

Oxford BioChronometrics SA

January 2015

Abstract

We present the results of research to determine the ratio of Ad-Clicks that are human initiated against those that are initiated by automated computer programmes, commonly known as ad-bots. The research was conducted over a 7 days period in early January 2015, using the advertising platforms of Google, Yahoo, LinkedIn and Facebook. The results showed that between 88 and 98 percent of all ad-clicks were by a bot of some kind, with over 10 per cent of these bots being of a highly advanced type, able to mimic human behaviour to an advanced extent, thus requiring highly advanced behavioural modelling to detect them.

1 Introduction

In May 2014, according to the Financial Times[1] newspaper, part of a Mercedes-Benz on-line advertising campaign was viewed more often by automated computer programmes than by human beings. It was estimated that only 43 per cent of the ad impressions were viewed by humans. Later, in December, Google made a similar announcement[3] when it stated that its research has showed that 56.1 per cent of ads served on the Internet are never "in view". From our own informal research using existing data from detecting spam-bots, it was thought that the level of bots involved in ad fraud might be considerably higher than was being generally reported. Consequently, we set out to conduct a controlled experiment to answer the following questions:-

1. What is the ratio between ad-clicks charged for, ad-clicks from bots and ad-clicks from humans, and
2. How many different types of ad-click bots can we observe.

2 Internet Bots - what we know

According to Wikipedia[4], an Internet bot, also known as web robot, WWW robot or simply bot, is a software application that runs automated tasks over the Internet. Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone. The largest use of bots is in web spidering, in which an automated script fetches, analyses and files information from web servers at many times the speed of a human. Each server can have a file called robots.txt, containing rules for the spidering of that server that the bot is supposed to obey or be removed.

In addition to these uses, bots may also be implemented where a response speed faster than that of humans is required (e.g., gaming bots and auction-site robots) or less commonly in situations where the emulation of human activity is required, for example chat bots.

There has been a great deal of controversy about the use of bots in an automated trading function. Auction website eBay has been to court in an attempt to suppress a third-party company from using bots to traverse their site looking for bargains; this approach backfired on eBay and attracted the attention of further bots. The United Kingdom-based bet exchange Betfair saw such a large amount of traffic coming from bots they launched a WebService API aimed at bot programmers through which Betfair can actively manage bot interactions.

Bot farms are known to be used in online app stores, like the Apple App Store and Google Play, to manipulate positions or to increase positive ratings/reviews while another, more malicious use of bots is the coordination and operation of an automated attack on networked computers, such as a denial-of-service attack by a botnet.

Internet bots can also be used to commit click fraud and more recently have seen usage around Massively Multiplayer Online Roleplaying Games (MMORPG) as computer game bots. A spambot is an internet bot that attempts to spam large amounts of content on the Internet, usually adding advertising links.

Bots are also used to buy up good seats for concerts, particularly by ticket brokers who resell the tickets. Bots are employed against entertainment event-ticketing sites, like TicketMaster.com. The bots are used by ticket brokers to unfairly obtain the best seats for themselves while depriving the general public from also having a chance to obtain the good seats. The bot runs through the purchase process and obtains better seats by pulling as many seats back as it can.

Bots are often used in MMORPG to farm for resources that would otherwise take significant time or effort to obtain; this is a concern for most online in-game economies. Bots are also used to artificially increase views for YouTube videos. Bots are used to increase traffic counts on analytics reporting to extract money

from advertisers. A study by comScore found that 54 percent of display ads shown in thousands of campaigns between May 2012 and February 2013 never appeared in front of a human being.

In 2012 reporter Percy Lipinski reported that he discovered millions of bot or botted or pinged views at CNN iReport. CNN iReport quietly removed millions of views from the account of so-called superstar iReporter Chris Morrow. A followup investigation lead to a story published on the citizen journalist platform, Allvoices[2]. It is not known if the ad revenue received by CNN from the fake views was ever returned to the advertisers.

3 Generally observed behaviour

All bots have a common set of properties. It can be said that a bot:-

- primarily exists, directly or indirectly, for economic gain,
- mimics, to any extent, the actions of a human using a computer,
- repeats such actions multiple times,
- initiates activity,
- executes only the minimum necessary actions to complete its task.

Bot behaviour, at the atomic level, falls into any one the following general classifications (*with examples of type*):-

1. Sends a single message (*Denial of Service Bots, Distributed Denial of Service Bots, Ad Click Bots, Ad Impression Bots*),
2. Sends a single message and waits for response (*Email Spam Bots, Ad Click Bots, Ad Impression Bots, Online Banking Bots*),
3. Sends multiple messages asynchronously (*Denial of Service Bots, Distributed Denial of Service Bots*),
4. Sends multiple messages asynchronously and waits for one or more responses (*Online Spam Bots*).

In behaviours 2 and 4, the sender address (i.e. the IP Address) must be valid for the response to be received (although not necessarily the point of origin), while behaviours 1 and 3 can accomplish their task without this prerequisite condition, making them considerably harder to detect their true point of origin.

4 How the research was conducted

In order to limit the level of non ad-platform bot activity being recorded, individual web pages were created specifically as the click target for the ad, one per ad platform. HTTP GET logging software was enabled for each of these web pages, recording each HTTP GET request that was made to the web server. Embedded on each of the target web pages was a JavaScript library, providing data collection functions to the web page. These functions were designed to record:-

1. Device-specific data, such as the type of web browser being used by the device, predetermined calculations to estimate CPU capabilities, hashing of HTML CANVAS elements to determine screen resolution, etc.

2. Network-specific data, such as the geo-location of the ip address, determining if the ip address was a proxy server, details of the DNS used, fixed-size data packet transmission latency tests, etc.

3. Behaviour-specific data, such as when and how the mouse and keyboard were used for devices that raise mouse and keyboard events, while for mobile devices, recording the data from the gyro, accelerometer and touch screen events.

Each of the three data sets that were being collected from the web page, were sent to their own separate web server using a variety of transmission methods. These were:-

1. Creating an empty SCRIPT Document Object Model Tag element, setting the SRC attribute to the URL of a collection script and parsing the collected data as a HTTP GET parameter.

2. Creating an new IMG Document Object Model Tag element, and again setting the SRC attribute to the URL of a collection script and parsing the collected data as a HTTP GET parameter.

3. Creating a Document Object Model HTTPRequest instance (also known as an AJAX request) to post the data to a collection script on the same server from where the web page was loaded.

Including the server HTTP GET request logs, this gave us in total four streams of data, which were relatively independent of each other, providing us with the ability to create much richer models of ad-bot behaviour and enabling us to create thoroughly-researched ad-bot classifications.

The advertising platforms used were Google, Yahoo, LinkedIn and Facebook. The ad-click budget allocated was around £100 (GBP) per platform, which was the maximum lifetime budget for the ad campaign and was used as fast as possible on each platform.

5 Types of ad-fraud bot detected

While observing the behaviour of bots, we were able to create six classifications of bot types, that we propose as a class of the Kouwenhoven-Neal Automated-Computer-Response Classification System and are described thus:-

Basic - (Ad-Clicks Only) Identified through the difference between the number of Ad-Clicks charged by a specific ad platform, and the number of consolidated HTTP GET requests received for the unique URL that was designated as the ad-click target for the ad campaign running on the ad platform.

Enhanced - Detected through the correlation of a HTTP GET request received by an ad-server for a specific ad, with the AJAX-transmitted record of the web-browser load event. If the recorded load event is inconsistent with the standard load event model, the HTTP GET was made by a bot.

Highly Enhanced - Detected through the use of advanced JavaScript processor metrics. A bot is evident if the client-side code execution is inconsistent with known code execution models.

Advanced - In an elementary attempt to impersonate human behaviour, the page is loaded into the web-browser, but the combination of the length of time that the page is supposedly viewed and the subsequent number and type of supposed user activities show very high levels of inconsistency with our models of normal human behaviour.

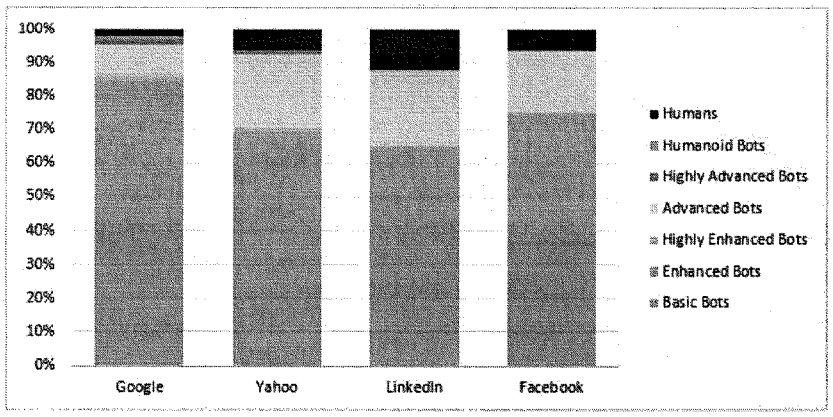
Highly Advanced - A significant attempt at impersonating human behaviour, the bot views the page for an amount of time that would seem reasonable. Both mouse and keyboard events are triggered and the page might be scrolled up or down. However, using cluster analysis, the pseudo randomness is highly detectable.

Humanoid - Detected only through deep behavioural analysis with particular emphasis on, for example, recorded mouse/touch movements, which may have been artificially created using algorithms such as Bezier curves, B-splines, etc., with attempts to subsequently introduce measures of random behaviour, mimicking natural variance.

6 Results

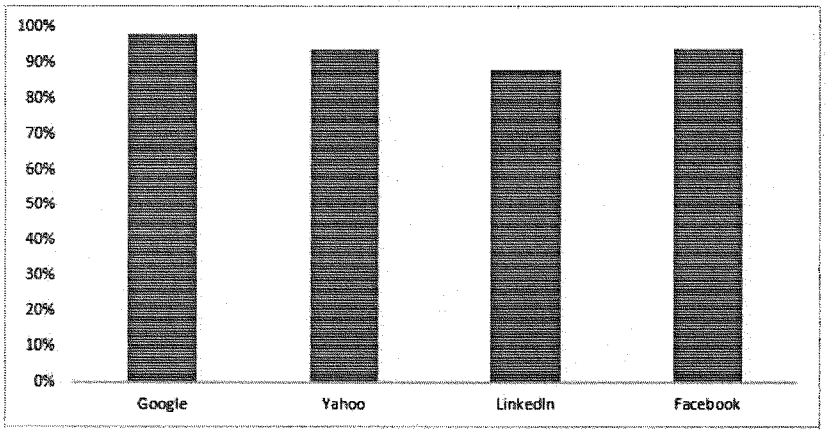
Our research found that at best, 88 percent of the ad-clicks were made by bots on the LinkedIn ad platform, while at worst, 98 percent were from bots on the Google ad platform.

Figure 1: Ratio of Ad-Bot Clicks to Human Clicks



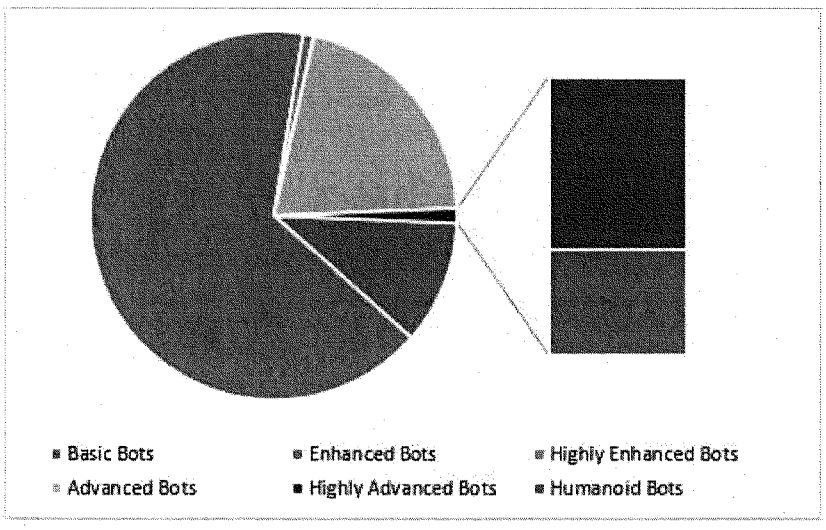
There were no instances where we were not charged for an ad-click that was made by any type of bot.

Figure 2: Prevalence of Overcharging of Ad-Clicks



The prevalence of the different types of ad-bot was not entirely as expected. We expected that the majority of bots would be of the basic type and that they would diminish in a linear fashion as they became more advanced. This was not the case, as the Enhanced bot was by far the most widely observed, with the second being the Advanced bot.

Figure 3: Types and Prevalence of Ad-Bots



The limited sample size and duration of this test notwithstanding, these findings are in keeping with our general observations of bot activity through conventional bot detection software, which analyses Internet traffic as a whole on a post real-time basis.

7 Conclusion

There are perhaps few industries where overcharging on such a scale as demonstrated here would be tolerated, but until very recently, the ability to model both human and bot behaviour at the necessary level of complexity (and thus hold advertising platforms to account) was not commercially feasible.

However, with the rise of what is commonly referred to as Big Data, the ability to collect, store and process vast amounts of data in real-time at reasonable cost, while modeling complex human (and human-like) behaviour, has fundamentally changed the balance of power in the relationship between advertisers and the advertising platforms.

References

[1] R. Cookson. *Mercedes online ads viewed more by fraudster robots than humans.* Financial Times, 2014.

[2] Percy Lipinski. *CNN's iReport hit hard by pay-per-view scandal.* Allvoices, 2013.

[3] Z Wener-Fligner. *Google admits that advertisers wasted their money on more than half of internet ads.* Quartz, 2014.

[4] Wikipedia. *Internet Bots.* Wikimedia Foundation, Inc., 2015.

AD FRAUD SUMMARY

OXFORD BIOCHRONOMETRICS analyzes millions of web interactions and ad views per day. Based on our advanced algorithms we can determine the behavior of each visitor and device to determine whether the interaction is a human or an automated script appearing to be a human (i.e., a bot). Our false positives and false negatives are under one percent despite the fact that bot technology is constantly evolving.

Bots are attracted to digital ads and websites for a variety of reasons. The biggest abuses are driven by financial gains for the players involved - the bot operator, the publisher of the website, the network, the ad agencies and other participants in the chain. The business model generally is quite simple across the board. Fees are charged per event and the more events that are logged the more money that can be charged. The following are some examples:

- **Publisher Fraud** occurs when a website publisher purchases bot to view their own site. This allows them to charge advertisers for each view or click even though they know that they created the interaction and that it did not come from a human. Other participants in the chain participate in the cash flow stream and nobody has an incentive to complain. The website now has significant revenue from fake views. They are financially motivated to continue this fraud because the revenue exceeds the expense of operating the bots and the risk of being prosecuted is thought to be low.

- **Social Network Fraud** occurs because networks (particularly a "closed garden" variety) are paid to reach a wide number of individual consumers. The more members there are in a social network (even if the operator of the network knows many are bots) the more advertising revenue it will attract. These networks also have the ability to command a premium because of the perceived quality of their user base.

- **Geo fraud** occurs when an advertiser wants to purchase a specific number of ads per day in a particular region. Unfortunately, the agency or network provider can't find enough spots in that location to purchase. As a result, the ads are displayed, against the instructions of the client, in other parts of the world. This is a rapidly growing issue in many parts of the world, particularly in high income, low population areas. For example, a local car dealer might request that all ads be displayed within a 20-mile radius of the dealership. The problem is that the ads are deliberately shown to people (and bots) around the world and will never help the dealer sell more cars. Unfortunately, the dealer will never know about the wasted advertising money without the use of sophisticated analytics.

- **Viewability Fraud** occurs where an ad is shown improperly such as behind a webpage and is invisible to the person viewing the real website and include:
  - **stack fraud** where ads are placed one on top of the other making most invisible;
  - **1x1 fraud** where the ad is reduced to one pixel by one pixel;
  - and a variety of other forms with the goal of packing the most number of ads into a webpage, such that as each ad is reported as viewed, increasing the revenue of the bot operator.

Bot operators are attracted to ticket vendors, travel sites, news sites and many others to scrape data and resell services, provide price comparisons, purchase items and force delays, spam and commit credit card fraud.

Who pays for all this ad fraud?
The end consumer. And the Retail Investor.

Advertisers overpay for their digital ads by $16.4 billion per year according to a study commissioned by WPP. We believe this study may actually understate the costs that are ultimately passed on to consumers and retailers. As the problem grows it imposes a significant hidden business tax. Participants in the digital ad ecosystem have clear motivation to return higher revenue and exceed quarterly expectations. By utilizing non-human traffic to view, click, like, link or join it can become very easy for the unscrupulous to earn illegitimate revenues. If those revenues were used to promote and support public investment, then ad fraud quickly can become a securities fraud issue.

A common misperception is that ad fraud is committed only by criminal networks (and perhaps the Russians). However, ad fraud is much more widespread than that and is committed willingly by a large group of otherwise honest participants in the advertising ecosystem who fall into the non-human dependent trap.

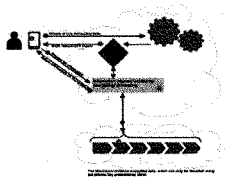
We believe that publishers and ad networks that charge advertisers for bots to view ads have defrauded the advertiser. We also believe that a social network or web operator that knowingly or willingly accepting non-human "members" has defrauded the public and their clients. While some percentage is due to faulty IP address lists, cookie misusages, bot created artificial cookies, VPN and ad blocker usage or errors in location services, the bulk is the result of intentional deception to produce additional revenue.

OXFORD UNIVERSITY INNOVATION

UNIVERSITY OF OXFORD

About Us

From our inception at the Oxford University Innovation Center OXFORD BIOCHRONOMETRICS has sought to provide the highest level of security without invading personal privacy. We will continue to build upon our proprietary technology to solve these problems, and to tackle related issues as they arise.

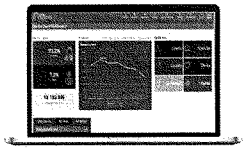


Our Technology

We believe that enormous opportunities in e-Commerce, digital advertising and publishing inevitably attracted nefarious players to the internet. Spam, "fake news," ad fraud, credit card theft and a corresponding loss of privacy have permeated the ecosystem on which we all rely. Policy questions include: how do you balance the good from the bad? What's the level of fraud or privacy invasion that's acceptable? We believe the answer is none.

We have developed proprietary Human Recognition Technology, (HRT) that creates a unique biometric authentication mechanism HRT+ for anyone – or *anything* – that interacts with our embedded code. OXFORD BIOCHRONOMETRICS' HRT determines definitively which interactions are human-derived and which are not, with independent studies having validated that our technology catches more fraud than alternatives that

represent the current standard. Our technology is so advanced that NATO announced OXFORD BIOCHRONOMETRICS as a winner of the agency's 2017 Defense Innovation Challenge, characterizing the technology as "transformational and state-of-the-art."



Our Solutions

Digital Media Solutions are OXFORD BIOCHRONOMETRICS products that identify non-human (bot) digital advertising fraud - these tools and services empower advertisers to ensure publisher traffic integrity and to pay only for traffic that matters.

- **SecureAd** Suite of products;
  - **SecureAd** Impressions
  - **SecureAd** for Search
  - **SecureAd** for Video
  - **SecureAd** for Agencies
  - **SecureAd** for Advertisers

Cyber Solutions are OXFORD BIOCHRONOMETRICS products that prevent fraud from happening.

- **SecureForm** (formerly **NoMoreCaptchas),** thousands of websites globally using this product to prevent spam and to block invalid user activity.
- **SecureLeads** uses Oxford BIOCHRONOMETRICS' Human Recognition Technology to verify that a human has filled out a lead/contact/signup form.
- **Secure Checkout** detects non-humans interacting with payments pages and blocks attempts at fraudulent credit card purchases.

Data

For the purpose of this report we will look at real data from a number of our clients that we have made anonymous. The selection covers the U.S., U.K., Norway, Belgium, Germany and Switzerland. All of the clients in the sample use at least one form of security to prevent bots and are targeted for distribution within the originating country.

Country	Bots	Humans	Total	%Bots
US	3,782,717	13,034,627	16,817,344	22.5%
UK	32,126,263	366,026,545	398,152,808	8.1%
Norway	1,049,077	6,603,516	7,652,593	13.7%
Germany	2,822,968	29,319,801	32,142,769	8.8%
Switzerland	1,314,620	26,989,945	28,304,565	4.6%
Belgium	7,538,878	39,879,307	47,418,185	15.9%

Our first pass shows the percentage of bots by the selected countries, but please note that as our business is largely based in Europe, that US data set is much smaller than the EU. OXFORD BIOCHRONOMETRICS will update the results as we get more US based data. In any event globally we see bot fraud at an average of 9.1 percent non-human traffic.

Next, we look at geo fraud

Country	In Target	Out of Target	Total	% Geo Fraud
US	14,572,400	2,244,944	16,817,344	13.3%
UK	391,338,470	6,814,338	398,152,808	1.7%
Norway	7,351,192	301,401	7,652,593	3.9%
Germany	31,138,234	1,004,535	32,142,769	3.1%
Switzerland	25,679,394	2,625,171	28,304,565	9.3%
Belgium	45,489,334	1,928,851	47,418,185	4.1%

The US again leads the way. These data show all activity, bot and human with the displayed ads and websites. The average geo fraud is 3%. For Switzerland, we included surrounding countries in the target calculation, thus potentially understating this fraud type.

Combining the two fraud types starts to show the bigger picture. Remember we are not yet calculating the other fraud types mentioned or hijacking.

Country	Bots and Geo Fraud	Relevant Humans	Total	Total Fraud
US	5,500,364	11,316,980	16,817,344	32.7%
UK	38,073,030	360,079,778	398,152,808	9.6%
Norway	1,126,311	6,526,282	7,652,593	14.7%
Germany	3,722,277	28,420,492	32,142,769	11.6%
Switzerland	3,701,305	24,603,260	28,304,565	13.1%
Belgium	9,090,290	38,327,895	47,418,185	19.2%

12% of all views are considered to be fraud, which easily supports the independent studies claiming the loss of $16.4 billion to ad fraud, with Statista claiming the 2018 total ad spend of $268 billion.[1] However, based on this small sampling, just these two simple frauds can claim up to $32.16 billion per year.

Where are these bots coming from?

Country	In Target Bots	Out of Target Bots	Total	% Out of Target
US	3,255,420	527,297	3,782,717	14%
UK	31,258,692	867,571	32,126,263	2.7%
Norway	824,910	224,167	1,049,077	21.4%
Germany	2,717,742	105,226	2,822,968	3.7%
Switzerland	1,100,436	214,184	1,314,620	16.3%
Belgium	7,161,439	377,439	7,538,878	5.0%

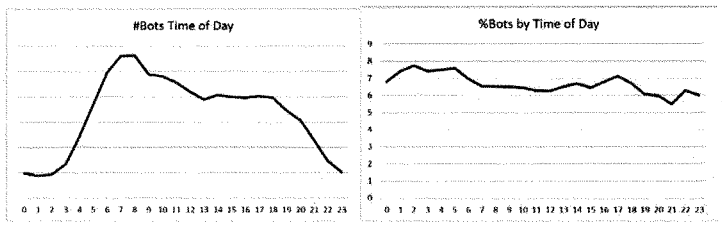
The vast majority of bots come from within country and are not external attacks.

How are these bots attacking?

device	Humans	Bots	total	
car	449	705	1,154	61.1%
desktop	131,332,627	6,966,538	138,299,165	5.0%
game console	32,613	2,671	35,284	7.6%
laptop	2,052,556	51,410	2,103,966	2.4%
phone	23,578,222	2,003,900	25,582,122	7.8%
smarttv	37,839	6,228	44,067	14.1%
tablet	13,503,425	770,846	14,274,271	5.4%

From the chart above you can see that desktops remain the most prevalent platform for the delivery of bots. However, phones have a higher percentage and mobile ad fraud is positioned to grow. It is interesting to note that bots claiming to be from cars and smart TVs have a growing percentage of activity (over 300 percent increase since the third quarter of 2017) and we can imagine it will only increase with the increase of the Internet of Things (IoT), it would be natural to speculate that IoT like smart coffee makers and refrigerators will make our list before too long.

When are these Bots attacking?



While the absolute number of Bots correlates to general human working hours, the percentage correlation is more evenly distributed.

Summary

The fraud reported here is just a small slice of the overall fraud. Policy makers should keep in mind that it generally comes from domestic sources rather than foreign agents and is distributed amongst a wide range of platforms. Ad fraud is constantly evolving.

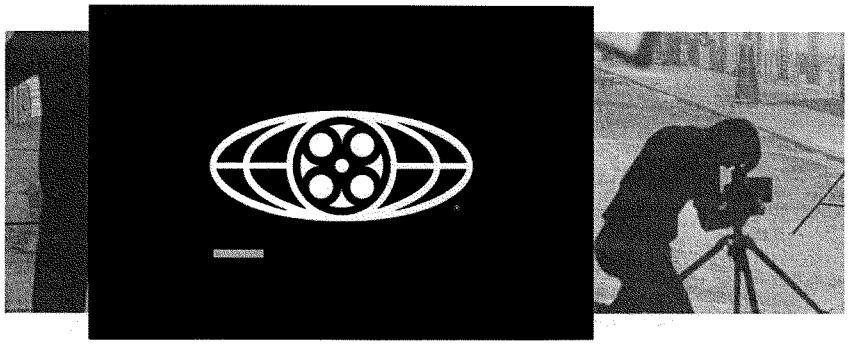
In a future report, we will update our evolution of bots to show how the simple spam bots of the past, that are easily measured now by most ad fraud detection companies, are decreasing and more humanoid bots, that browse websites, create a history, are able to fill in forms and simulate mouse movements, are becoming more prevalent.

Older generation technology has moved from protecting the advertiser and consumer to protecting the networks, agencies and publishers. Nonetheless, these same companies and groups claim that fraud is decreasing. What is decreasing is their ability to detect the continually advancing threats. While our solutions cannot entirely prevent fraud, we can report and audit very effectively. In our experience, clients actively using our prevention techniques and use the data to remove outliers continually see improvements and reduce the price of the hidden tax.

Constant vigilance, best of class fraud detection and remediation will help to reduce ad fraud and associated costs to consumers and businesses. All players in the market need to be held accountable – networks, agencies, demand side and supply side platforms and publishers – but it must start with the advertisers themselves to demand accountability and proper auditing.

---

[i] Digital advertising spending worldwide from 2015 to 2020 (in billion U.S. dollars), statistica, https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/.



Voluntary Advertising Initiative May Hold a Key to a Responsible Internet

JUNE 14, 2018

BY NEIL FRIED

If I told you the advertising industry might hold a key to saving the internet, you'd probably say I'd downed one too many Old Fashioneds with Don Draper. But stick with me. A House Digital Commerce and Consumer Protection Subcommittee hearing today entitled *Understanding the Digital Advertising Ecosystem* may make things a little clearer.

Advertising—including digital advertising—is an essential way to support and distribute compelling and diverse content. As we are all aware, however, the internet is also increasingly riddled with illicit activity, from child sex trafficking to rogue pharmacies, identity theft to theft of intellectual property, and fake news to malware. Unfortunately, online advertising supports those endeavors, too. This intersection of advertising and the seedier side of the web creates problems for everyone, albeit solvable ones.

Ad agencies, ad brokers, websites, and advertisers see financial and reputational harm to their businesses when legitimate advertising is connected to disreputable content.

This is perhaps best evidenced by YouTube's recurring problem of placing clients' ads next to terrorist propaganda, hate speech, and sexually inappropriate content. Online advertising also funds illegal activity, including content theft, with criminal enterprises collecting hundreds of millions of dollars a year from ad-supported piracy, for example.

Sometimes the advertising is itself nefarious, such as "malvertising" that infects computers and spawns botnets, or "click fraud" that artificially inflates a site's revenues and steals from advertisers. According to the Interactive Advertising Bureau, ad-related clickfraud, piracy, and malvertising cost the U.S. digital marketing, advertising, and media industries $8.2 billion a year, and that doesn't include the cost to consumers, which may be even higher.

The good news is that one of the witnesses at today's hearing, Trustworthy Accountability Group President and CEO Michael Zaneis, is helping to fight harmful and illicit online activity through a collaborative, private-sector initiative between the advertising and content communities. As his written testimony explains, TAG seeks to combat fraud, malware, and piracy while promoting transparency and rebuilding trust in the internet. It brings together companies from across the digital advertising ecosystem to keep good ads off bad sites.

This is by no means a simple task. Much work remains to be done, and TAG can only help steer advertising away from unsavory sites when advertisers actively participate in the process. But if legitimate advertisers refuse to place ads on harmful and illicit sites, and if reputable sites refuse to accept ads from less than reputable sources, the internet will be a better place. Bad actors will have less revenue, legitimate sites will be easier to distinguish from disreputable ones, and the web just might be a little more civil.

TAG is just one of several important initiatives in this space. Payment processors such as Mastercard, Visa, and Paypal are working to prevent bad actors from using their financial networks to collect revenue from unlawful online activities. Amazon and eBay

have measures to keep counterfeit goods, piracy devices and applications, and other harmful or illicit products off their online marketplaces.

Other online platforms and internet intermediaries would do well to better emulate these types of voluntary initiatives, especially in light of growing scandals. Unfortunately, many continue to resist overtures for such cooperative problem solving. By acting responsibly and collaboratively to keep digital neighborhoods safe for communication, commerce, and creativity, online platforms and internet intermediaries could help ensure we realize the vision we all have for the internet.

READ FULL ARTICLE ONLINE: https://bit.ly/2Msgiiv

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

July 13, 2018

Ms. Rachel Glasser
Global Chief Privacy Officer
Wunderman
3 Columbus Circle
New York, NY 10019

Dear Ms. Glasser:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Thursday, June 14, 2018, to testify at the hearing entitled "Understanding the Digital Advertising Ecosystem."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions by the close of business on Friday, July 27, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Janice D. Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

WUNDERMAN

July 26, 2018

Chairman Robert E. Latta
House of Representatives
Subcommittee on Digital Commerce and Consumer Protection
2125 Rayburn House Office Building
Washington, DC 20515-6115

Chairman Latta,

Thank you for your follow up to the hearing entitled "Understanding the Digital Advertising Ecosystem" before the Subcommittee on Digital Commerce and Consumer Protection held on June 14, 2018.

Enclosed in this letter please find my responses to your follow up questions. I have also emailed a copy Ali Fulling at Ali.Fulling@mail.house.gov.

Please do not hesitate to reach out if I can be of further assistance. I am honored to help in the education and understanding of the digital advertising ecosystem, as it is a complex space that is vital to the internet economy, free internet, and free access of content.

Thank you.

Sincerely,

[redacted]

Rachel Glasser
Chief Privacy Officer
Wunderman

3 Columbus Circle, New York, NY 10019 T+212-941-3257

July 26, 2018

Rachel Glasser
Responses to Additional Questions for the Record "Understanding the Digital Advertising Ecosystem"

To Chairman Robert E. Latta
Subcommittee on Digital Commerce and Consumer Protection

1. As a board member to the NAI, what are the NAI guidelines and prohibitions relating to interest based advertising or cross app advertising directed to children under 13 years old?

The NAI Code prohibits creation of personalized advertising segments targeted to children under 13 years old without verifiable parental consent. ["Use Limitations" Section II.D.1 of the NAI code: "Members shall not create Personalized Advertising segments specifically targeting children under 13 without obtaining verifiable parental consent."]

Further, the NAI Code requires member companies to comply with all applicable laws and regulations. The Children's Online Privacy Protection Act (COPPA), and the COPPA Rule, amended July 1, 2013, (16 CFR 312) further prohibits collection of Personally Identifiable Information (PII) (including persistent identifiers) from children under the age of 13 without verifiable parental consent.

NAI commentary (also found in the Code, page 22) states that NAI member companies must comply with the FTC's Children's Online Privacy Protection Act (COPPA) rules, as such rules may be updated from time to time. During the NAI's most recent full annual review (2017), no NAI member reported knowingly collecting or using data of children under the age of 13 for Personalized Advertising purposes.

2. Can you explain in detail how the NAI's opt-out feature works and how opt out preferences are recalled across a consumer's browsers and devices? Do participating companies still collect data from users that opt-out for purposes other than interest-based advertising or is data collection prohibited altogether?

The NAI offers Internet users the ability to opt-out of interest-based advertising on the web from NAI members. The opt-out works by setting an "opt-out cookie" per member either in place of, or in addition to, cookies that a member company uses to identify a device. While this opt-out cookie is present on a browser, member companies stop delivering interest-based advertisements to that browser and do not collect data for the purposes of interest-based advertising. The NAI centralized opt-out works by connecting a user's browser to hundreds of special URLs set up by the member companies that use the connection to set their own optout cookie and ensure that they can read it. This functionality is checked by the NAI regularly to

ensure that each member's integration is working as expected, in addition to ongoing technical health checks.

Participating companies may still collect data from users that opt out for purposes other than interest based advertising. One such purpose may include analytics or the ability to understand how users interact with a specific site or app. This data tends to be in aggregate, (or non-personal) and helps identify content to be delivered to users (e.g. 20% of browsers viewed article X after viewing article Y). Data is collected to prevent fraud, such as determining which traffic is likely an automated bot attempting to defraud people. This data is important for other purposes such as security (e.g. identifying suspicious login attempts) and frequency capping (so a user does not see the same ad thousands of times).

3. It has been suggested by others that many ad tech companies prefer not to identify consumers by name or other, non-anonymous information for interest based advertising or cross app advertising. "Most ad tech companies don't want to know the identity of a consumer for IBA. Please elaborate why this is the case?

Member companies, and non-member companies for that matter, have significant reasons for not collecting consumer's PII. First, holding data that can specifically identify individuals poses liability and reputational risks in the event of unauthorized access or a data breach. Second, the NAI Code requires heightened protections for the use of PII, and disincentivizes the collection and use of PII through strict requirements. Use of PII also typically will require more rigorous security protocols, heightened legal obligations, liabilities, more intensive employee training, and other issues. Third, ad tech platforms that do not use PII are able to deliver effectively targeted ads using non-PII in a hashed or encrypted format, or some sort of identifier like a cookie or ad id. Finally, ad tech platforms are encouraged and incentivized by the NAI Code, general best practices, and risk mitigation and liability concerns to implement data minimization procedures.

4. Zuckerberg argued consumers have control of their data and FB does not "sell" consumer data. The practical issue is many parties in the digital advertising ecosystem may join or connect their own consumer data and information with Facebook's data or vice versa. What self-regulatory measures have been or should be implemented to enhance integrity and transparency of the joining and sharing of consumer data between and among entities who may hold 1P information and entities who hold 3P information?

The NAI has created and enforces several relevant Code provisions to enhance the integrity and transparency of the data ecosystem.

First, any NAI member that receives user level data from another party is required by the NAI Code to require *that* party to have an appropriate privacy notice and choice provision. NAI Code II(F)(2).

Second, if an NAI member is collecting or using data on a first party's website, that first party is required to have an appropriate privacy policy which includes a disclosure that personalized advertising may be occurring on the site, a description of the types of data collected on the site, an explanation of any data transfer to third parties, and a conspicuous link to an opt-out mechanism for personalized advertising. NAI Code II(B)(3-4).

Third, the NAI requires opt-in consent for retrospective merger of PII and Device-Identifiable Information (DII) for Personalized Advertising purposes. NAI Code II(C)(1).

Fourth, if an NAI member shares DII with a third party, that third party must be contractually prohibited from merging the DII with PII or attempting to otherwise re-identify the individual for Personalized Advertising purposes without opt-in consent, unless the data transferred is proprietary data of the receiving party.

Fifth, NAI members may not allow the use of Personalized Advertising data for any of the following purposes: employment eligibility, credit eligibility, health care eligibility, and insurance eligibility and underwriting and pricing.

5. Devices listening: what are the self regulatory rules the NAI has in place or intends to implement to enhance transparency and disclosure by ad tech companies which have access to audio data [GR3] from smartphones, voice assistants, and similar devices that consumers do not know is being collected about them?

The NAI Code is technology agnostic: if audio data is used for personalized advertising purposes it is covered by the NAI Code. During the NAI's most recent full annual review (2017), no NAI member reported collecting microphone data for personalized advertising purposes. In addition, the NAI is always updating the Code to keep pace with technology, and may issue guidance or code updates to clarify the Code's application to specific technologies.

a. Following up: are any mobile phone, voice assistance and smart TV manufacturers members of the NAI? If not has the NAI had any discussions with these types of OEMs about potential concerns relating to the use of audio and data files?

Yes, there are several members of the NAI that engage in personalized advertising based on certain types of television data. In addition, NAI members frequently consider new business opportunities, and engage the NAI about best privacy practices for emerging technologies and novel data types. One product of these efforts is the NAI's advanced TV guidance released in July 2018, which covers the use of audio/visual data.

i. Which causes you greater concern, that our devices may be listening to us or that digital models are so accurate that they can predict what we want without listening to our conversations?

There are many things that concern me when it comes to some new technologies and applications of such. Both items outlined in the question are concerning – While presently there has been more attention in the news media paid to data practices, like digital models, I am personally more concerned with devices that may be listening to our conversations. I feel strongly that there should be easy "off" buttons, and heightened security controls as we have seen some unintended sharing of information from listening devices over the last year or so. (An Amazon Alexa sending a recorded conversation to a contact in the device owner's contact list; being used as evidence in a murder trial, if you ask Siri how to turn it off, you will constantly get vague answers. It does not tell you to go to your settings or what to do once you are there.)

Additionally, I'd like to note the difference between modeling, which is about *predictions* of ads which is often a best guess and not a known fact, vs devices that actively or even passively listen to end users.

One big concern when it comes to listening devices is consumer expectation. Do you expect your TV to listen to you for the purposes of advertising? Perhaps now the answer is no, but this can change in the future as technology and our behavior change and evolve. on the converse, perhaps a user would expect a voice activated remote control to listen when a voice command is provided to the remote. User behavior and expectations change over time. Nearly 20 years ago we likely would not give out our personal photos or postal address. Now these pieces of information are posted online by users to participate in things like social media, and networking, voluntarily exposing their information to the public and/others.

Companies like mine recognize these concerns and it's not in their interest to act in this way by engaging with practices that are so contrary to consumer expectation.

Finally, I believe I spoke along these lines at the hearing, however to emphasize, I strongly believe that there is the need for consumers to better understand how ads work, and I strongly believe that there should be more educational efforts all around.

6. In Carpenter v US, a 5 justice majority noted "a cell phone faithfully follows it owner beyond public thoroughfares and into private residence, dr. offices political HQ, and other potentially revealing locales. Do consumers have enough information about what data, including location data, is being gathered about them from phones and wireless devices?

I think this can depend on context. For example, use of precise location data for the purposes of advertising requires an opt-in, and location services can be shut off and permissioned by the user at the device and app level. However, cell tower data collection (as was at issue in Carpenter) cannot be turned off. Further Carpenter had an issue of life and liberty at stake, so the court's ruling that collection of data in excess of seven days constitutes a "search" is understandable.

I'd also point to the recent US v Jones (132 S.Ct. 945 (2012)) decision held that installing a GPS tracking device on a vehicle and using the device to monitor the vehicle's movement

constitutes a search under the Fourth Amendment, is similar in its holding in that systematic monitoring or surveillance of individuals is not permissible without a warrant. While Jones has a vehicle and GPS at issue and Carpenter a cell phone which may be viewed as inherently more personal, (ie, most people will not take their car with them to the restroom...) one can argue that a car follows the user just the same as a cell phone does.

To me this indicates that although many of our laws were written and codified before much of this technology and its application was ever contemplated, our courts recognize some of the nuance and intrusion this type of data can impose when used improperly.

Further, sharing location data for personalized ads, by comparison, is opt-in and under self-regulatory codes cannot be used for credit/health eligibility decisions, let alone Constitutional questions.

7. Some have suggested that larger mature ad tech companies will have the resources to comply with GDPR and in fact may benefit greatly from the law's implementation. What evidence if any, are you seeing that ad tech companies are pulling out of the EU, or moving towards consolidation, in the aftermath of GDPR implementation?

There is at least one NAI member company that has publicly announced that they are no longer doing business in the EU as a result of the implementation of the GDPR. Other NAI member companies have indicated that their revenue in the EU has dropped significantly because of the GDPR, and those NAI members that are continuing to do business in the EU have expended significant resources in pursuit of GDPR compliance.

Perhaps an impact not contemplated or argued enough is the point that there are many publisher sites who perceive the risk of non-compliance with the GDPR as too high, and as such have limited access to the content on their site. This is done so that users trying to access the site from the EU are unable to, protecting the site owner from processing EU personal data, and preventing their services from targeting the EU arguably bringing them out of scope of the GDPR. This has a potentially chilling effect on the availability of free content and access to free content for people of all socioeconomic backgrounds, as companies may have to block access altogether, limit advertising reducing revenue, and implement paywalls to make up for that lost revenue. The free internet now becomes a paywall. This is a much larger impact we will only begin to recognize once it is too late.

8. In 2015, the IAB launched LEAN ads program and the CBA. Di LEAN and CBA arise as a direct response to user's concerns relating to tracking and privacy, the use of ad blocking software or both? In your estimation, based on any studies or empirical evidence in the public domain since 2015, have these initiatives been successful in allaying fears about privacy or the rise of ad blocking?

There are several more recent empirical studies that say that the primary reasons people install ad blockers are the annoyance factor of ads, and the negative consumer experience created by

invasive ads, including the use of data to deliver negative ad experiences. The Coalition for Better Ads addressed this problem by identifying ad formats with the lowest levels of consumer approval through statistically robust surveys, and then taking measures to discourage the use of these ad formats (e.g. full-screen takeovers).

- First, there are studies that say people install ad blockers because they think ads are annoying, instead of for privacy reasons:
  - IAB - https://www.iab.com/wp-content/uploads/2016/09/IAB_Research_AdBlocking_Consumer_Survey_11.16.pdf
  - NAI - http://www.networkadvertising.org/blog-entry/nai-consumer-survey-digital-advertising-online-content-and-privacy/
- Second, tailored ads provide ~3x more value to publishers than generic ads, so publishers are able to reduce the number of ads per page by using personalized advertising. - http://www.aboutads.info/resource/fullvalueinfostudy.pdf
- Third, economics research has shown that a publisher can choose one of two routes to rely on ad revenue: ads can either be tailored and unobtrusive, or they must be generic and obnoxious. Tailored advertising reduces the number of obtrusive ads seen by consumers. (Tucker). - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600288

9. In Google's privacy policy, the company explicitly states it may combine information we collect among our services and across your devices...depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google. Technically how does Google or another firm join different sets of personal data collected on different affiliated or non-affiliated sites or apps?

Technically they (data activation & data marketplaces – non-walled garden eco-system, or third parties) do not *generally* join personal data from different data sets collected from sites or apps to each other in the manner hypothesized. Rather they may join non-personal data tied to a device identifier (which can be reset and/or shut off by the user). These firms adhere to defined best practices as set forth by the FTC and privacy initiatives, and industry models. These are codified in their audited declarations reviewed by groups like the NAI, DAA and IAB.

Companies like Google, Twitter, or Facebook, (walled gardens) are login based. These companies use the user login, like an email address, as the persistent identifier by which they link other cookie or ad IDs. For example, if a user logs onto Facebook using their laptop and their Google Chrome browser, Facebook will log a cookie on the chrome browser used on that device that is linked to the user's login ID or email address in this case. User logs out, and goes to a different nonaffiliated website (wwww.xyz.com). The original cookie (linked to the user ID) will register the nonaffiliated website, (xyz.com), the user went to after they logged off from Facebook. Alternatively, if the page or site has a Facebook button, this too can be used to link the user (although this is specific to Facebook, but can be the case for other social widgets or buttons). On a mobile device, the persistent identifier used may be the user's login, it can also be the device phone number if such information is provided by the user. Think of this in the

context of Gmail and the scale of individuals who have a Gmail account and use the Gmail app to login.

For clarity however, and to points made earlier in this document, Self-regulatory codes require that these data collection, use, and merger policies are disclosed at the time of collection. This is usually done either in the site or app's privacy policy, or in the form of "enhanced notice". The NAI code as discussed earlier has specific requirements if this data (PII and non-PII/DII) is to be merged. Within this framework firms will make data associations that are compliant with the data collection and management policies and industry guidelines.

These disclosures and acting in accordance with these disclosures brings websites and apps under the FTC's section 5 Authority of deceptive and unfair trade practices.

a. What other stakeholders in the digital ad ecosystem have access to 3P data and can firms with 3P data that is not directly embedded and connected to the ecosystem join their data with firms that are embedded and connected?

Typically, stakeholders wishing to participate in the digital data ecosystem and utilize 3P data from embedded and connected firms need to activate their data into a pseudonymized format. To initiate this, they must validate that the data they wish to associate has been sourced and adequately permissioned and that they have rights to this. (for example, did the privacy policy disclose this use of the data when the data was collected)? They will then utilize a specialist activation service which creates a pseudonymous ID that enables connection to the eco-system but restricts the capability to make the connections personally identifiable.

b. Are there specific types or categories of stakeholders who have no consumer information or data in their possession for the purposes of facilitating the serving or display of online ads?

If I understand the question correctly, then yes, some advertisers, publishers, and networks do this. This is a great example to demonstrate how diverse the digital advertising space is. Very few entities see much of the puzzle. Some advertisers simply say, "please make sure 100k different people see this ad." Some companies specialize in only hosting ad images. Some companies only help fight bot-fraud, some companies only predict weather. And some are prohibited for collecting this type of data for use in behavioral advertising depending on the context (for example, COPPA. Also, contextual advertising is permitted, provided it meets certain standards. Contextual advertising also does not collect persistent IDs, or gather information about a user's visits across websites over time. Contextual advertising places ads based on the content on the web page). There are many stakeholders who have no consumer data for the purposes of serving ads.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

July 13, 2018

Mr. Mike Zaneis
President and CEO
Trustworthy Accountability Group
888 17th Street, N.W., Suite 620
Washington, DC 20006

Dear Mr. Zaneis:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Thursday, June 14, 2018, to testify at the hearing entitled "Understanding the Digital Advertising Ecosystem."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions by the close of business on Friday, July 27, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Janice D. Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

[Mr. Zaneis did not answer submitted questions for the record by the time of printing.]

Additional Questions for the Record

The Honorable Robert E. Latta

1. What criminal activity in the digital advertising supply chain is most worrisome to you?

2. What upcoming steps is the digital advertising industry considering and implementing to fight against criminal activity?

3. In 2017, P&G marketing chief Marc Prichard described the digital media supply chain as "murky at best and fraudulent at worst." It's a provocative statement for sure. Over about the last 25 years, as the ecosystem has increasingly gathered more data, honed automation, and established better analytics, why is the digital advertising ecosystem not functioning better? Similarly, what can be done to give stakeholders and consumer greater confidence in digital advertising?

4. Is it fair to assert that any ad-click made by a non-human is fraudulent? If so, why is it difficult to detect and combat against? What is the percentage breakdown of ad-clicks charged for, between ad-clicks from bots and ad-clicks from humans?

5. In June 2018, at the annual ad Festival in Cannes, France, Unilever marketing chief Keith Weeds called social media influence marketing, "[a]t best it's misleading, at worst it's corrupt. . .[for] the sake of a few bad apples in the barrel, I believe there is risk in the area of influencers."[1] The practice of padding follower counts with fake accounts and bots is pervasive, as the consultancy Points North Group found that midlevel influencers—those with between 50,000 and 100,000 followers—often have about 20% fake followers and that North America "brands pay influencers millions of dollars each month to reach follower [sic] that are fake."[2] Can you elaborate on what are the specific harms associated with this practice of deceptive misrepresentation?

6. What has been the impact of the use of ad-blockers to fight against criminal activity? Are consumers using ad-blocking options on their PCs and smartphones, as well as new innovations like voice assistants and smart TVs? How do advertisers, agencies, and others adjust and respond to the impact of ad blocked inventory, and what impact do ad-blockers have on revenue opportunities for websites?

7. In 2015, the Interactive Advertising Bureau launched the "LEAN" Ads Program, LEAN" translating to Light, Encrypted, AdChoices supported, Non-invasive ads. In 2016, leading trade associations and companies involved in online media joined forces to create the Coalition for Better Ads (CBA). Did the LEAN Ads program and CBA arise as a direct response to users' concerns relating to tracking and privacy, the use of ad blocking software, or both? In your estimation, based on any studies or empirical

[1] Suzanne Vranica, "Unilever Demands Influencer Marketing Business Clean Up Its Act," *Wall Street Journal*, June 18, 2018, at https://www.wsj.com/articles/unilever-demands-influencer-marketing-business-clean-up-its-act-1529272861

[2] *Id.*

evidence in the public domain since 2015, have these initiatives been successful in allaying fears about privacy or the rise of ad blocking?

8. What are the top 5 global ad providers (in terms of revenue) in the digital advertising ecosystem? What are the top 5 global browser firms for both worldwide desktop browser usage or market share, as well as worldwide mobile browser or app usage or market share?

9. Can ad-blocking rules and techniques be used for competitive advantages in the digital advertising ecosystem? Can such rules and techniques be used to disadvantage and discriminate against particular companies, ads, contents and voices?

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

July 13, 2018

Mr. Justin Brookman
Director
Privacy and Technology Policy
Consumers Union
1101 17th Street, N.W.
Washington, DC 20036

Dear Mr. Brookman:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Thursday, June 14, 2018, to testify at the hearing entitled "Understanding the Digital Advertising Ecosystem."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions by the close of business on Friday, July 27, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Janice D. Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

ConsumersUnion®
THE ADVOCACY DIVISION OF CONSUMER REPORTS

Responses of **Justin Brookman**
Director, Privacy and Technology Policy
Consumers Union

to the Questions for the Record of Ranking Member Janice D. Schakowsky relating to

The House Subcommittee on Digital Commerce and Consumer Protection hearing on

Understanding the Digital Advertising Ecosystem

July 27, 2018

1. I have heard from many in industry that regulations have the potential to further entrench the control large players have on the market at the expense of small business. Specifically, instead of leveling the playing field for small business to compete with companies like Facebook and Google, privacy regulations could make it harder for small business and exclude them from the market altogether. How do you respond to that argument?

I think that the notion that privacy protections will entrench Google and Facebook is belied by the fact that Google and Facebook have consistently lobbied aggressively against nearly all proposed privacy legislation in both the United States and Europe. I heard similar arguments that adoption of Do Not Track would favor those companies; again, however, both fought hard to stop industry adherence to that standard. As a result, Google and Facebook (and the vast majority of the ad tech industry) ignore users' DNT instructions on the web to this day.

Certainly, if a company's business model is predicated entirely on bad privacy practices, than privacy legislation will especially impact them, and will probably disadvantage them more compared to companies like Google and Facebook. Both companies have problematic practices that should be addressed by privacy rules, but both also have core products that can be monetized effectively without compromising user privacy. However, because those companies' business models are also heavily reliant on the use of personal information, privacy law does impact them directly — and more than most companies. The Federal Trade Commission has brought actions against both companies for privacy violations, though due to weaknesses in the law and the limitations in its own authority, its actions have not sufficiently deterred their abuses.

Effective privacy law should not simply mandate expensive processes and compliance programs. Fundamentally, privacy law should accord behaviors with consumer's reasonable expectations; if a small business is not engaged in dubious data practices, it should not be impacted by new privacy protections as much as a larger player like Google or Facebook.

2. *At the hearing, Mr. Beales suggested that when we try to regulate data collection, we need to focus on potential harms. He implied that we should only limit data collection or use when it results in harms to consumers.*

a. Do you agree with Mr. Beales? Please explain why or why not.

I would respond by pointing out that the collection of information by another invariably carries with it a *risk* of future harm. As I argue at more length in the paper *Why Collection Matters*,[1] once collected, data may always be used in subsequent ways adverse to the interest of the individual: it may be breached to the public, accessed and misused by company employees, or put to a future unwanted use by the company itself (such as tailored price discrimination designed to extract the maximum consumer surplus from any transaction). Any user may rationally want to limit data collection forestall those risks. As such, I am not entirely sure that I disagree with Mr. Beales' premise so much as his constrained assessment of consumer risk (or harm).

b. It seems to me that our options for purchases or deals we may be offered can vary thanks to mass data collection and targeted advertising, resulting in some people being given bad choices or bad deals. Is that a valid concern? What are some of the potential consequences to consumers of data collection and targeted advertising that may not result in legally provable damages.

Yes, this is a valid concern. Or rather, there are two separate concerns here: first, some consumers may be getting offers for inferior products due to unfair assessments made by a targeting algorithm. For example, although credit decisions are governed by the Fair Credit Reporting Act, a decision to market certain credit cards to certain individuals probably is not. A company may make an unfair assessment that a particular individual is a significant credit risk based on bad assumptions or bad data — as a result she may receive an offer for a credit card with a higher interest rate than other similar customers.

Second, data collection and increased informational imbalances may allow companies to engage in individualized pricing, whereby they may have increased capacity to offer the highest possible price a person would be willing to pay for a particular product or service. Given the

[1] https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf

rise in corporate concentration in recent years, these types of practices are more likely to be effective, given that consumers may have fewer market alternatives for any given product.

One sector that very likely uses first degree price discrimination is the travel and airline industry. Since 2000, Consumers Union has been investigating the murky pricing practices by airlines and travel companies online, and reporting on disturbing evidence of bias in how airfares are presented to the public. In recent years some of these marketing schemes have come to light, particularly after the International Air Transport Association — the global airline industry's leading trade organization — unveiled "New Distribution Capacity," a detailed program to enhance "product differentiation."[2] A recent study commissioned by an aviation company reported the airlines are developing "dynamic availability of fare products" that "could be adjusted for specific customers or in specific situations."[3]

In October 2016, Consumer Reports published an extensive study of nine leading travel sites and compared identical itineraries in real time using both "scrubbed" browsers cleared of all cookies and browsers used for extensive web searches.[4] Among 372 searches, we found 42 pairs of different prices on separate browsers for the same sites retrieved simultaneously. Industry representatives dismissed them as technological glitches. In previous years, Consumers Union found similar evidence of pricing based on search histories with airlines and other products and services. In March of 2018, Consumers Union endorsed Senator Chuck Schumer's call for the Federal Trade Commission to investigate the airline industry amid questions about the use of "dynamic pricing" and consumers' personal online data to set the price of airfares, which Schumer termed "a sad state of affairs that just might violate consumer protections."[5]

However, these practices are not restricted to the travel and airline industry. Uber and Lyft are both believed to engage in individualized pricing, though their criteria for doing so are not transparent.[6] A recent report from Deloitte and Salesforce finds that 40% of brands that currently use artificial intelligence to personalize the consumer experience have used this technology to tailor prices and deals in real time.[7] And these practices are obscured to the end user by design. According to Maurice Stucke, professor of law at the University of Tennessee,

---

[2] https://www.iata.org/whatwedo/airline-distribution/ndc/Pages/default.aspx.
[3] https://www.atpco.net/sites/default/files/2017-10/ATPCO%20PODS%20Dynamic%20Pricing_2.pdf.
[4] https://www.consumerreports.org/airline-travel/how-to-get-the-lowest-airfares/.
[5] https://consumersunion.org/news/consumers-union-praises-senators-call-for-ftc-investigation-of-airline-dynamic-pricing/.
[6] https://consumersunion.org/news/consumers-union-praises-senators-call-for-ftc-investigation-of-airline-dynamic-pricing/.
[7] https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/e-books/learn/consumer-experience-in-the-retail-renaissance.pdf.

information about first-degree pricing practices typically "only comes out when there's a leak, when someone from the inside divulges it."[8]

3. The General Data Protection Regulation recently went into effect across the European Union. People have raised concerns that the new rules will negatively affect the effectiveness of advertising and will, they argue, hurt business. This concern about the economic effects of privacy regulation on industry is not new. At study from 2011, cited in the Majority's hearing memo, seemed to find that advertising effectiveness was lower in Europe, which was subject to a different set of privacy regulations at the time, than in other parts of the world. Do you have any comments about that study? How concerned should we really be about the economic effects of privacy regulation.

The 2011 study cited in the hearing memo suffers from serious limitations that make it very difficult to broadly extrapolate that privacy laws would lead to a "65 percent decrease in ad effectiveness." First, the study did not attempt to measure whether participants made more or fewer purchases in response to an ad; instead, it only registered survey results as to whether users who took a ten-minute survey reported that they were likely or not to buy a particular product for which they had seen an ad. More fundamentally, the study does not actually look at what — or even whether — ad tracking and targeting practices changed as a result of the enactment of the e-Privacy Directive in Europe. Europe at that time already had privacy law (the Data Protection Directive) in effect (notably, under the Data Protection Directive, the study found advertising to be *more* effective in Europe than outside of Europe, though the authors do not dwell on this finding). Although the study vaguely states that the e-Privacy Directive was more rigorous, it also notes that some practitioners did not believe that consent rules were meaningfully affected by the Directive. Indeed, it is because of perceived limitations in the ePrivacy Directive that Europe subsequently enacted the General Data Protection Regulation and is currently considering a new ePrivacy Regulation. And notably, industry guidance around targeted advertising in Europe after the enactment of the ePrivacy Directive roughly matched comparable guidance in the United States.[9] Absent *any* details about how or whether European companies (particularly the ones associated with the survey) altered particular practices in response to that Directive — as well as any data about the particular ads shown to users — it is difficult to summarily rely on the stated sentiment analysis revealed by the survey.

That said, any lawmaker should be concerned about the economic consequences of regulation, including privacy regulation. Privacy laws that broadly constrained legitimate practices to which few users object could well be harmful for the economy and would not meet

[8] https://www.theguardian.com/commentisfree/2018/apr/13/uber-lyft-prices-personalized-data.
[9] https://www.edaa.eu/wp-content/uploads/2012/10/2013-11-11-IAB-Europe-OBA-Framework_.pdf.

consumers' needs. On the other hand, users should not be asked to accept unfettered intrusion into their lives all in the name of economic efficiency and making advertising more relevant. User well-being and autonomy may justify the prohibition of certain invasive practices, or at least affording users with some choices over data collection and use. Even if this does result in some reduction in the efficiency of ad targeting (for which many users have strongly expressed a preference), it would be beneficial for the long-term health of the ecosystem, as failure to address privacy concerns has led to the rapid rise in the adoption of ad blockers (presumably less targeted advertising is still considerably more effective than no advertising at all).[10]

4. Advertisers can micro-target ads by choosing specific categories of people they want to market to. But by choosing who they want to advertise to, advertisers are also excluding others. That can make sense. You want to advertise products to the people that are most likely to purchase them. But I want to explore what happens when certain groups are excluded from seeing certain ads.

a. Please provide some examples of when targeted advertising has been explicitly or implicitly used to discriminate.

Here are a few recent examples of where targeted advertising has had an (in many cases, likely inadvertent) effect:

- Researchers at Carnegie Mellon found that women were less likely to be shown Google ads for high-paying positions compared to men.[11] A subsequent study similarly found that women were less likely to receive advertisements about STEM careers even though the ad was targeted as gender neutral; the study found that because women are generally a more attractive demographic than men for other advertisements, it was cheaper to serve the ads to a larger male audience.[12]
- Facebook has allowed advertisers, including those who are advertising housing, to intentionally discriminate on the basis of race, disability, parenthood, and sex (they are currently being sued in the state of New York).[13] On Tuesday, Facebook

[10] https://www.nytimes.com/2017/01/31/technology/ad-blocking-internet.html.
[11] https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study.
[12] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852260.
[13] https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin; https://motherboard.vice.com/en_us/article/43bxq9/facebook-sued-for-discriminatory-ad-targeting-housing-propublica.

signed a deal with the state of Washington to stop third-party advertisers from preventing protected groups from seeing their ads.[14]

- Latanya Sweeney demonstrated that stereotypically African American names were more likely to generate ads suggestive of an arrest than a search of a stereotypically white name (regardless of whether the company placing the ad reveals an arrest record associated with the name).[15]

Leading academic researchers have also sought to quantify the potential for discrimination in online ad targeting.[16]

b. It has been reported that Facebook's advertising categories allow people advertising jobs to exclude older people from seeing the ads. A Facebook spokesman said, "used responsibly, age-based targeted for employment purposes is an accepted industry practice." Is age-based targeted for job ads really a common industry practice?

I do not have any special insight into how common age-based targeting is. However, plaintiffs in a recent class action suit over age-targeting on Facebook have alleged that T-Mobile, Amazon, Cox, and "hundreds of other companies" targeted various job advertisements only at younger demographics.[17]

c. What can we do about this problem? Would it help to prohibit the collection and use of data that identifies people as being part of legally protected classes or otherwise vulnerable populations, or is that too easily worked around because inferences can be made from all the other information collected?

At the very least, requiring more transparency around data collection and targeting practices can help bring more accountability to companies' practices. Some companies — including Google and Facebook — have taken positive steps in making information available about ad profiles and why certain ads are shown, though progress has certainly not been uniform. I am not convinced that comprehensive prohibitions on targeting based on legally-protected classes are appropriate, as advertisers may have legitimate and societally beneficial reasons for marketing particular products or services specifically to say, women or senior citizens. However, some prohibitions — including around the use of proxies as substitute for protected classes — are certainly needed. There are open questions about how anti-discrimination laws that were enacted before the age of digital platforms and widespread automated decision-making do or should apply to today's practices. There is already a robust

---

[14] https://www.reuters.com/article/us-facebook-advertisers/facebook-signs-agreement-with-washington-state-to-end-discriminatory-ad-targeting-idUSKBN1KE2RX.
[15] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208240.
[16] http://proceedings.mlr.press/v81/speicher18a/speicher18a.pdf.
[17] https://www.vox.com/policy-and-politics/2018/5/31/17408884/facebook-amazon-job-ads-age-discrimination-lawsuit.

discussion taking place on how to ensure fairness in algorithmic targeting;[18] I encourage this committee to further explore these questions as well as the broader questions around algorithmic accountability.

5. We often hear from the advertising industry that the information they collect is anonymous. But there are companies that sell what some call onboarding services. These services link offline consumer data with online users by matching identifying information collected offline — like when you give your email address at a stores' checkout — to the same consumers online — like when you use your email address to log in to some websites.

a. These companies operate behind the scenes, without consumers even realize who those companies are or what they are doing. As you pointed out in your testimony, most tracking methods are unobservable. Is there any way to a consumers to find out which companies have used onboarding services?

Unfortunately, it is very difficult for even extremely savvy consumers — or technical researchers for that matter — to determine which companies supplement online data with offline information. While nearly all publishers have privacy policies, few have detailed information about practices such as onboarding, and anyway consumers cannot reasonably be expected to read and digest dozens of such policies per day (see Answer 11 below). Very advanced consumers can research the different types of third-party tracking companies and then use extensions such as Ghostery to see which are embedded into which websites — though even then they may not necessarily know which of a tracking company's services are being used in any instance.

When I worked at the Federal Trade Commission's Office of Technology Research and Investigation, we were able to detect some online publishers transmitting login credentials in raw or hashed form to a variety of third parties, though it was not evident whether that was done in order to facilitate onboarding, cross-device tracking (see Answer 7 below), some other functionality, or was just a product of poor site design.[19] And if companies transmitted identifying information in less observable methods, we would not have been able to detect the behavior at all.

b. Is there any way a consumer can opt-out of this type of hidden practice. And even if a consumer could opt out at some later point, hasn't the damage already been done?

As discussed in more detail below (see Answer 8), while industry self-regulatory programs offer users opt-out choices, those opt-out have fundamental weaknesses — most

[18] https://fatconference.org/.
[19] https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf

notably, they do little to address underlying data collection practices and primarily only limit use of certain data for ad targeting purposes. Users can try to limit sharing email addresses with online publishers, but that would prohibit them from taking advantage of many sites' primary functionality. An advanced user could use an email management service such as Abine to generate service-specific email addresses. For most users however, the simplest solution is to use a tracker blocking extension such as Disconnect.me, uBlock, or EFF's Privacy Badger. These extensions prohibit publishers from transmitting identifying information to third parties through the web browser (though they may still find other methods to share identifying information off-line). If a user does inadvertently allow identifying information to be transmitted to a third-party, there may be no way to disassociate historical data with such identifier, but deleting cookies and prospectively blocking trackers should limit companies' ability to associate future online behavior with offline data tied to that email address (though companies may use other, non-cookie methods to maintain state on a user).

c. We have repeatedly heard advertisers claim that consumers' identifies are not attached to data collected about them. How easy or difficult is it to re-link a consumer's identity to a detailed profile about him or her?

First, the talking point that online tracking is "anonymous" is less frequently used than it once was. While the FTC's 2001 closing letter over DoubleClick's merger with Abacus helped to establish industry practice to divorce online behavior with real-world identifiers,[20] for many companies, that prohibition has fallen by the wayside. Most notably, Google and Facebook now associate user behavior across the web and in other apps with login identity. Moreover, industry self-regulatory codes do not prohibit tying behavioral data to real-world identifiers such as name and email address. Some companies may tie browsing behavior to a hash of an email address; this provides a speed bump against reidentification but can in many cases be easily circumvented.[21] Even if behavior is merely tied to a pseudonymous cookie and IP address, identification may be possible, especially by the ISPs who assign IP addresses, and who in recent years have made aggressive advances into the ad tech space.

d. What is the effect of a breach of an onboarding company on consumers, who do not even realize their information was being collected by this company?

It depends on how the onboarding company — or a company who has onboarded offline information — stores its data. If extensive logs of web history are stored with an email address or other persistent identifier, that would be very problematic. While I do not know if "onboarding" companies store data this way, other companies — such as Google and Facebook — tie cross-site and -app behavior to login credentials; a breach of this data would reveal

---

[20] https://www.ftc.gov/sites/default/files/documents/closing_letters/doubleclick-inc./doubleclick.pdf.
[21] https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous.

tremendously personal (and potentially embarrassing, or even dangerous) information about consumers' online behavior (in academic studies, Google and Facebook have been shown to track users across the considerable majority of other websites and apps through, *inter alia*, their deployment of analytics and advertising code, and social sharing and login widgets).[22] And as discussed above, even if behavioral data is only correlated with hashed identifiers, it may be trivial to reassociate that data with actual consumers if additional steps are not taken.

e. Are there other concerns about linking a consumer's behavior offline with that consumer's online behavior that you want to mention?

In general, consumers' expectation is that they surf the web anonymously unless they log into certain services — and even then, they don't expect their login information to be shared with third-parties. From the adage "On the internet, nobody knows you're a dog" to ad tech's historical insistence that online tracking was "anonymous," consumers do not expect — and many reject — efforts to tie their online behavior to offline identity. Failure to respect consumer expectations and preferences — and the context in which data is provided — may result in further backlash against industry, and may also create a chilling effect on online behavior. A fear of persistent and uncontrollable tracking — and negative consequences therefrom — should not dissuade consumers from seeking out information on potential health conditions or other sensitive issues.

6. As we explored during our Facebook hearing, an advertiser can target specific people with a specific ad. Instead of targeting a category such as women in their 20s who like shoes, an advertiser can hand Facebook the names of 20 individuals and send a specialized ad just to them. While we have heard that Facebook and Google do not sell information, this targeting option certainly does not suggest anonymity. Could this type of harassment of specific names lead to harassment and other concerns?

Yes, while Facebook and Google technically do not "sell" information, they make tremendous amounts of money in selling targeting based on users' personal information, even if they are careful to prevent third parties from accessing the data. Online targeting by real world identifiers such as email address and telephone number is becoming more common — not just by Facebook and Google, but by other companies that gain access to your personal information, either because you provided it to them (such as your ISP or cable company) or because they received it from a partner.

I do not know each company's minimum size audience for this type of targeting, though given the challenges in screening ad content, I agree that the potential for abuse certainly exists — especially if minimum audiences are small. In the world of geolocation targeting, we have

---

[22] https://webtransparency.cs.princeton.edu/webcensus/; https://techscience.org/a/2015121502/; https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf.

seen very small target areas allowed — such as patients visiting health facilities[23] and employees in a single government office building.[24]

In any event, even if this type of targeting is allowed, at the very least companies should offer usable tools to stop this type of targeting. However, many do not. Facebook, for example, offers a custom audience tool that displays which companies have uploaded your contact information for ad targeting and gives you the ability to delete each one. However, you can only see twenty companies at a time, and you are forced to delete each one individually instead of globally (and prospectively) opting out of custom targeting.

7. Many data collectors seem to be focused on collecting as much data as possible. Beyond their web browsing, consumers are being tracked across many of the devices they use, like smartphone, tablets, desktop computers, and Smart TVs. Companies often use this data to personalize advertising, and to make assumptions about their future behavior.

a. Are consumers aware that their activity on their smartphone, for example, is being linked to the shows they watch on their smart TV or the books they read on their tablet?

I am not aware of any studies that specifically explore consumer awareness around cross-device tracking. However, given the consistently poor disclosures around these types of behaviors, I would be very surprised if there was significant awareness of how consumers are tracked across separate devices. Even as a researcher trying to quantify the amount of cross-device tracking, I was unable to conclusively determine the extent of cross-device tracking on 100 popular websites: often data was collected and shared that *could* be used for cross-device correlation, but it was unclear from company disclosures whether the data was in fact used for that purpose.[25]

b. Are we being tracked across devices even if we, the users, do not take any action to link those devices.

Yes. First, some actions we may not think of opening us up to cross-device tracking may in fact do so. By logging into services like Google and Facebook on multiple devices, you give those companies the ability to track your behavior across most other websites and apps. A new app might include software designed to use your microphone to listen in the background for ambient TV shows or music.[26] And even if we you never provide identifying information and

---

[23] https://www.npr.org/sections/health-shots/2018/05/25/613127311/digital-ambulance-chasers-law-firms-send-ads-to-patients-phones-inside-ers.
[24] https://splinternews.com/how-a-senator-used-facebook-ads-to-influence-employees-1793856310.
[25] https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf.
[26] https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html.

only use web browsers to passively surf content, companies may make probabilistic inferences about device correlation based on shared IP address and geolocation, and commonality of browsing history and behavior.

8. The advertising industry has assured us that it provides consumers the opportunity to opt out of targeted advertising through the Digital Advertising Alliance and the Network Advertising Initiative, which are industry self-regulatory bodies. But these opt-outs have limitations.

a. Does the opt out mean that a person will no longer get targeted ads at all?

The scope of industry association opt-outs are defined by their own terms, but none would prevent *all* targeting. Certainly, contextual targeting (based on the present site visited) would not be prohibited by any opt-out, though few privacy advocates object to that practice. However, other forms of personalized targeting may still be allowed. For example, the Network Advertising Initiative 2018 Code of Conduct requires an opt-out to stop targeting based on other sites or applications visited.[27] However, users may still be targeted by other attributes, including demographic data (possibly obtained through onboarding) or geolocation.

b. It is my understanding that a consumer can only opt out of the targeted advertising, but not the data collection. Do you agree? Does opting out of targeted ads mean a consumer will stop being tracked?

Industry opt-outs are primarily focused on limiting certain forms of targeting — they do not meaningfully limit data collection and retention. A person using an industry association opt-out for targeted ads will still be tracked. And while some codes — such as the Digital Advertising Alliance's Self-Regulatory Principles for Multi-Site Data purportedly include limitations on collection, the permitted rationales for data collection (including "market research" and "product development") as so broad as to effectively render the limitation meaningless.[28]

c. It is my understanding that DAA and NAI use the cookies placed on your browser to stop the targeted ads. So, if you clear your cookies, you are no longer opted out. Do you agree?

Yes, the primary method that DAA and NAI use for opting users out of web tracking is a persistent opt-out cookie. If those opt-out cookies are deleted, than the opt-out will no longer be recognized. DAA does offer a browser add-on designed to make user opt-outs persist even if

---

[27] https://www.networkadvertising.org/sites/default/files/nai_code2018.pdf.
[28] https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/Multi-Site-Data-Principles.pdf.

a user deletes their cookies.[29] However, information about this extension is not provided on the primary DAA opt-out page, and recent user reviews of the extension in the Google Chrome store report that the extension no longer works.[30]

d. As you pointed out in your testimony, there are many methods of tracking people that do not use cookies. Does that mean that even if you use an opt-out tool provided by the self-regulatory body and you do not delete its cookie, you could still be tracked?

Companies that participate in industry self-regulatory programs — even those who use non-cookie methods to track users — are required by the terms of those programs to honor opt-out cookies and limit the scope of ad targeting in response. Of course, as noted above, that opt-out does not address the underlying tracking for any companies, regardless of the methods they use. And companies that do not participate in these self-regulatory programs may continue to use cookies or other methods to track for whatever reasons they see fit.

e. Overall, are the opt-out tools offered by the industry effective?

No, as I explained in more detail in testimony before the Senate Commerce Committee several years ago, industry self-regulatory programs and opt-outs are insufficient:

- They only apply to trade association members,
- Cookie-based opt-outs are fragile,
- Industry opt-outs do little if anything to address underlying data collection and tracking, and
- Opt-out interfaces are clunky, and the controls often do not work: as noted, users have complained about the effectiveness of the DAA "Protect My Choices" extension, and requests to opt out of member tracking *en masse* on the DAA and NAI websites often result in dozens of opt-out requests failing.[31]

Today, due to the weaknesses in industry self-regulatory programs and the failure to honor user Do Not Track settings, the most effective solution to limiting online tracking is to install a tracker blocking extension such as Disconnect.me, uBlock, or Privacy Badger — or to use a browser that blocks tracking by default such as Brave (Safari and Mozilla also take steps to limit cross-site tracking as well).

---

[29] http://www.aboutads.info/PMC.
[30] https://chrome.google.com/webstore/detail/protect-my-choices/hdgloanjhdcenjgiafkpbehddcnonlic/reviews.
[31] https://cdt.org/files/pdfs/Brookman-DNT-Testimony.pdf.

9. You said in your testimony that "it is next to impossible for ordinary consumers to learn about how they are being monitored."

a. Members of the DAA and the NAI are required to put an icon on ads. Do those icons tell people how they are being monitored?

Even after nearly eight years, consumer awareness of the AdChoices icon remains low: the most recent available study pegged awareness at 33 percent.[32] For those users who do notice and click on the icon, they receive varying amounts of information about why any particular ad was delivered along with a link to an industry opt-out program (and in some cases, company-specific controls as well). In some cases, the information is extremely vague: for example: "Adobe cares about your privacy. We work with a number of companies that may use data about your online activity to show you relevant ads." In another case, I was told that an ad for a flight to Greece was based on "Google's estimation of your interests [and t]he time of day or your general location (like your country or city)." Sometimes the icon will simply direct to an advertiser's privacy policy, which is unlikely to provide meaningful, digestible information for most consumers. In cases of specific product retargeting, users are sometimes told specifically that the ad was shown because they had recently viewed those exact products on another site.

b. Members of the DAA and the NAI have a centralized industry website. Does the website provide sufficient information to tell people how they are being monitored?

The AboutAds resource that is often accessible from many AdChoices icon does provide a drop-down menu from which consumers can obtain some very high-level information about what interest-based advertising is.[33] The resource does not provide much detail about *how* users are monitored, though users can access other, more industry-facing, guidance on either the DAA or NAI site that may have more detail. However, I am unaware of an industry-created, consumer-focused primer on the various ways that consumer data is collected and shared for targeted advertising.

10. Online privacy in the United States is based on the concept of notice and choice. But we do not really have meaningful notice or meaningful choice. Most often, companies provide people with notice that their data is being collected and shared in their privacy policies and then given them the choice to use the product or not.

---

[32] https://www.mediapost.com/publications/article/318700/study-finds-few-americans-choose-adchoices-know-i.html.

[33] http://www.aboutads.info/how-interest-based-ads-work#aboutinterest.

a. Do you have concerns that individuals cannot choose to limit the collection of their data, not just from the website or advertiser, but from these opaque third parties that also get access to their data?

First-party data collection is generally fairly intuitive in web browsers, though for mobile applications that may have access to more device functionality, users may not always feel in control of what developers may have access to (though OS developers to their credit have iterated on ways to make this more transparent over the years). But users continue to express frustration with third-party data sharing, and as I highlighted in my original testimony, these tracking behaviors are becoming more sophisticated. Tracking blockers are fairly effective today in limiting data sharing, but this may simply force companies to share data server-to-server in ways that are difficult if not impossible to observe or control. Ultimately this arms race serves neither consumers nor industry, and privacy protections that clearly articulate user rights and choices are needed to mandate reasonable behaviors and set baseline expectations.

b. The digital advertising ecosystem has many players. Do you agree that consumers have no idea how many players there are or who they are?

Given the dizzying complexity of the digital advertising ecosystem,[34] I would certainly agree with your statement. Very few consumers are likely aware of companies such as Datalogix, Pulsepoint, and Pubmatic, nor could they differentiate the varying roles those companies play. Even for the companies they do know, consumers likely do not understand all the various ways that those companies collect information about them. For example, it is unlikely that most consumers understand that Google and Facebook track what users do off of their services on other websites and in other apps — and that that activity is logged with their real identity. I was gratified to see the recent Facebook hearings draw special attention to this issue.

11. Notice seems to be a flawed concept. How can I have notice of what information a company is collecting about me when I do not even have notice that there is a company in the first place? Moreover, a survey conducted by Professor Joseph Turow from the University of Pennsylvania found that more than 50 percent of internet users think that when a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users. Adding more information about third party collection to a privacy policy is not sufficient. Are current privacy policies working?

Privacy policies are certainly an ineffective method of providing information directly to consumers. Because the law does not clearly mandate specific disclosures, and because most

[34] https://lumapartners.com/content/lumascapes/display-ad-tech-lumascape/.

FTC privacy cases are predicated upon a specific misstatement in a privacy policy or elsewhere, privacy policies tend to be vague and expansive. But even if they were more precise, it would not be efficient for consumers to read them: a study by Aleecia McDonald and Lorrie Cranor estimated that reading every site's privacy policy would take users over 244 hours per year, at a collective societal cost in wasted opportunity of over $600 billion.[35]

I do think privacy policies have a role to play, however. I believe privacy law should require companies to provide more detailed information about their actual practices within their privacy policies — not for consumers, but for regulators, journalists, civil society, and ratings services such as Consumer Reports. As such, privacy policies would function more like financial filings, which are important accountability documents, and which are not necessarily read by ordinary investors, but which are processed by intermediaries to convey meaningful information to the marketplace.

Even with improved transparency, privacy law should not place all the burden on individuals to manage the collection and sharing of their personal information. Even mandating consent can be abused, as evidenced by the use of coercive "dark patterns" in response to the GDPR to manipulate users into broadly agreeing to a wide swath of opaque behaviors.[36] Certain broadly unacceptable behaviors should simply be prohibited — or possibly only allowed at the user's affirmative direction (as opposed to merely clicking "OK" to a consent box). For practices that are conducted on an "opt-out" basis, users need powerful, industry-wide opt-outs that let them make easy and manageable choices (such as "Do Not Call," or "Do Not Track" for that matter). Today's privacy framework in the U.S. puts too much burden on individuals to try to understand and control an increasingly complex and undecipherable array of behaviors.

---

[35] https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf.
[36] https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

July 13, 2018

Dr. Howard Beales
Professor of Strategic Management and Public Policy
George Washington University
Funger Hall
2201 G Street, N.W., Suite 615-P
Washington, DC 20052

Dear Dr. Beales:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Thursday, June 14, 2018, to testify at the hearing entitled "Understanding the Digital Advertising Ecosystem."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions by the close of business on Friday, July 27, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Janice D. Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

Answers to Questions for the Record

J. Howard Beales III

1. In your testimony, you mentioned companies like 33across and Accuen, which are not consumer facing but exist in the digital advertising space. How important are these ad tech businesses to the digital advertising ecosystem and how would regulation affect them?

Ad tech businesses are an essential part of the digital advertising ecosystem. A popular graphic of the marketing technology landscape from the Chief Marketing Technologist Blog by Scott Brinker includes more than 6,000 unique companies in 2018,[1] up from just under 5,000 in 2017. Many of these companies specialize in some specific piece of the process of connecting an advertiser and a publisher with an advertising availability, while others offer a broader range of services. There are demand side platforms, which aggregate demand from a range of participating advertisers, supply side platforms, which aggregate advertising offerings from participating publishers, and ad exchanges, which match bids from advertisers and demand side platforms with offerings from publishers and supply side platforms. In addition, there are companies that specialize in analytics, verification activities to assure that advertisements actually appeared as promised, data suppliers and aggregation, and performance measurement. Most of these companies are likely unknown to the overwhelming majority of consumers.

The entire chain of digital advertising market participants is most important to the smaller web publishers. My study with Dr. Eisenach found that although the largest web sites sell just under half their advertisements directly to the advertiser (and a comparable amount through third parties), the smallest websites in the study (ranked 4,000 by Quantcast in 2013) depend on third party mechanisms to sell roughly two thirds of the advertisements they display.

The impact of regulation depends on the nature of the regulatory requirements. In the chains of companies that link a particular advertiser to a particular advertising availability, each company in the chain handles the data about the consumer to whom the ad is to be delivered. If each company handling that data must obtain direct consent from the consumer, smaller companies that are not consumer facing likely could not survive. The problem would be similar if regulations required publishers or advertisers to identify all companies with whom they share data. The most likely result would be even more consolidation of the digital advertising market in the hands of market leaders, simplifying the consent problem but sacrificing an important and dynamic competitive element in the marketplace.

The identity of the companies in this value chain is, and should be, irrelevant to consumers. What is important is to prevent misuses of data or leakage of data in ways that could harm consumers. The same principle applies in other forms of transactions. There is no reason to think consumers need to know the names of every party through whom the details of their credit

[1] https://chiefmartec.com/2018/04/marketing-technology-landscape-supergraphic-2018/.

card purchase pass as it makes its way from the charge at a retail merchant to the bank that issued the card and sends the consumer a bill. Similarly, there is little reason to know or understand the parties involved between my request for money at an ATM and the bank that debits my account and authorized the machine to issue cash. It *is* important that information about my credit card or bank account number not "leak" to those who would misuse it, but asking the consumer's permission to share information with a particular intermediary will do virtually nothing to advance that objective.

2. Google's AdSense and AdWords, as well as Facebook's social plug-ins like the "Share" and "Like" buttons, appear to have widespread presence on the Internet. What competitive advantages does this give them in the digital advertising ecosystem as compared to other companies in the space?

Facebook's plug-ins are a source of competitive advantage because they enable the company to acquire information about their own users who visit those sites, as well as information about other consumers, whether or not they are signed in to Facebook. AdSense and AdWords, although they may create some competitive advantages, are also a reflection of the vast store of other information available to Google. More information generally enables better ad targeting, which is an important part of why many advertisers turn to Google. The large share of Google and Facebook in the digital advertising market makes competition from the smaller, more anonymous companies discussed above even more important.

3. Some have suggested that larger, mature ad tech companies will have the resources to comply with GDPR, and in fact may benefit greatly from the law's implementation? Do you believe this will be true?

Many of the costs of complying with the GDPR, or any other regulation, are essentially fixed costs. A new regulation often requires substantial resource expenditures to determine exactly what is required. Especially in software-driven systems, it also requires substantial programming expenditures to implement processes and procedures. These costs are largely independent of the number of transactions or the number of consumers who visit a website. Larger companies can spread these costs over a larger base, which may lead to a much smaller increase in average cost than the cost increase faced by a smaller company. The additional resources of a larger company are certainly an advantage, but the long term advantage is that regulation raises the per unit costs of smaller companies relative to larger ones.

A second critical advantage of some large companies in complying with the GDPR is that they are well known to consumers. To the extent that the rules require more explicit consent, consumers are more likely to give that consent to a well known company than to someone they never heard of and do not deal with directly. If they are unable to obtain consent when it is required, many behind the scenes players in the digital advertising market may disappear.

Media reports have also suggested that Google and Facebook have adopted stricter interpretations of the GDPR than are necessary, and that the effect of this stricter interpretation is

to disadvantage companies that are partners in some activities but competitors in others.[2] To the extent this is true, these companies may be using the regulation to create an artificial competitive advantage.

4. With the aim of enhancing consumer privacy, as compared to digital advertising effectiveness and return on investment, how helpful would meaningful data minimization or anonymization be in giving consumers greater control over data about them? What would that look like if businesses who collect consumer data had to implement minimization or anonymization? What are the trade-offs of placing restrictions on the secondary use of data?

Most data use in digital advertising markets is already anonymous. If anonymous browsing data is linked up with personally identifying information, it is most likely because a potential advertiser with whom the consumer has a specific account can match the account information to otherwise anonymous browsing information. In other contexts, such as medical information, anonymization is a useful tool than can enable secondary uses of data to address important research questions with substantially less risk that specific information can be tied to a particular individual.

Restricting secondary uses of data is particular problematic. In many cases, highly beneficial information uses are secondary uses: they are not the primary reason that information was collected initially. Many fraud control tools, for example, use information collected for a different purpose (such as credit reporting or marketing) to look for uses of personal information that are inconsistent with the way such information has appeared or been used in prior transactions. These inconsistencies indicate an increased likelihood that a transaction is fraudulent.[3] As another example, the availability of location information enables driving directions that take into account real-time traffic flows.[4] Digital mapping technologies, spam detection, instant spell-checking, and language translation tools are all useful services that were "after-the-fact data-driven innovations."[5] As the connected internet of things continues to expand, new and valuable secondary uses of data originally collected for another purpose are likely to expand, offering significant potential benefits.

Data minimization suffers from a similar problem. By definition, all secondary uses of information that is not retained (or is not collected in the first place) are precluded, however beneficial those uses might be. Moreover, it is difficult to define in any general way what information is "needed" for a particular service or transaction. If a requirement for data minimization is to be anything more than a generality, however, some such definition would be necessary. In general, there is no particular incentive for businesses to collect information that is not useful for anything. Moreover, there are incentives to destroy data that are no longer useful, particularly where the information is sensitive and loss or breach could create liability for the

---

[2] Google and Facebook Likely to Benefit From Europe's Privacy Crackdown, *Wall Street Journal*, Apr. 23, 2018
[3] See the discussion in J. Howard Beales III, Business Government Relations: An Economic Perspective (Kendall Hunt, 2nd Ed., 2012) at 112-113.
[4] See e.g. Waze Privacy Policy, https://www.waze.com/legal/privacy.
[5] Adam Thierer, Privacy Law's Precautionary Principle Problem, 66 Maine Law Review 467, 475 (2014).

company. If "minimization" precludes collecting or using information that is currently in use for other purposes, it could well preclude or undermine some useful information products or services.

○