NEAL R. GROSS & CO., INC.

RPTS SHIPLE

HIF165170

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, D.C.

The subcommittee met, pursuant to call, at 10:15 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, Cardenas, 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 & Investigations, Digital Commerce and Consumer Protection; Elena Hernandez, Press Secretary; Paul Jackson, Professional Staff, 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 five minutes for an opening statement. And again, good morning and I wanted to again thank our witnesses for being with 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 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 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.

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 gentle lady from Illinois, the ranking member of the subcommittee, for five minutes.

Ms. Schakowsky. Thank you, Mr. Chairman.

Ads are ubiquitous, often irritating, as you browse the internet. Most of the time, we get a 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, smart phone, 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 wising 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 five minutes.

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.

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 five-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 five 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, GLOBAL CHIEF PRIVACY OFFICER, WUNDERMAN; MIKE ZANEIS, PRESIDENT AND CEO, TRUSTWORTHY ACCOUNTABILITY GROUP; JUSTIN BROOKMAN, DIRECTOR, PRIVACY AND TECHNOLOGY POLICY, CONSUMERS UNION; HOWARD BEALES, PROFESSOR OF STRATEGIC MANAGEMENT AND PUBLIC POLICY, GEORGE WASHINGTON UNIVERSITY

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:]

**********INSERT 1**********

Mr. Latta. Well, thank you for your testimony this morning, and Mr. Zaneis, you are recognized for five 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 Brookman
Director, 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's 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 websites.

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 three 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 non-human 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:]

**********INSERT 2**********

Mr. Latta. Well, thank you very much for your testimony.

Mr. Brookman, you are recognized for five 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 seven 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:]

**********INSERT 3**********

Mr. Latta. Well, thank you again for your testimony.

And Dr. Beales, you are recognized for five minutes. Thank you.

STATEMENT OF HOWARD BEALES

Mr. 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 national advertising -- 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 Mr. Beales follows:]

**********INSERT 4**********

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 five 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.

768 And can you repeat the second part of your question?
769 Mr. Latta. Yes, and would you tell us also what kind of
770 information the digital ad businesses have about consumers and
771 how it's being used?
772 Ms. Glasser. Sure. Again, I think that also depends on
773 who you're speaking to in the supply chain. But, generally, for
774 a company like mine, the type of information that we usually hold
775 on the consumers would be things related to a cookie.
776 So that could include an IP address, cookie ID, browser
777 information. For example, if you're using a certain version of
778 Google Chrome or Internet Explorer, it might include a time stamp
779 and a date for verification purposes. It could really vary,
780 depending on how you set the cookie to collect information.
781 Mr. Latta. Thank you.
782 Mr. Zaneis, how significant of a problem are bots and fake
783 accounts in the digital ad ecosystem?
784 Mr. Zaneis. There's no question that it's a massive
785 challenge and a problem for the entire ecosystem. I think then
786 there's a recognition that no industry can be based off of this
787 high level of fraud.
788 The number that you quoted of 22 percent fraud in certain
789 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 two 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. Okay. 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 how much it would cost because that could really depend on --

Ms. Schakowsky. Mic.

Ms. Glasser. Sorry. It's my first time doing this.

[Laughter.]

Mr. Latta. It's fine.

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. Okay. Well, thank you. My time has expired and I will recognize the gentlelady from Illinois, the ranking member of the subcommittee, for five 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 five 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?

Mr. 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 --

Mr. Beales. Absolutely. Absolutely.

I mean, that -- 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?

Mr. 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.

Mr. 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 five 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. Okay. Okay.

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. Okay. How about you?

Mr. 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. Okay. 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 five 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 industry-wide 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 five 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. Okay. 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 yeah, 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 the -- 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 do 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 -- that's all that members are objecting to when -- 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, you know, here's how to do it.

It's just, like, a lot of labor, right. I mean, we all have -- we all got 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 five 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 labelled 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. I -- there is 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 three 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 five 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.

Mr. 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 five 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 four minutes you get a TV time out.

But I get to watch it for free because I got to watch the ad. And so -- and we are talking about free content. I think people 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.

Mr. 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 --

Mr. 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?

Mr. 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?

Mr. 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?

Mr. 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. Okay. 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 five minutes.

Mr. Cardenas. 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. Cardenas. 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. Cardenas. 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. Cardenas. 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.

1802 You know, how do you put in place, you know, because it is
1803 valuable, right. I mean, yeah, I suddenly need to pay -- spend
1804 a lot of money on the diamond ring right now.
1805 But I think people still wish they had autonomy and control
1806 over the things they own.
1807 Mr. Cardenas. Thank you. My time has expired.
1808 I yield back. Thank you, Mr. Chairman.
1809 Mr. Latta. I thank you very much. The gentleman's time
1810 has expired.
1811 The chair now recognizes the gentleman from Indiana for five
1812 minutes.
1813 Mr. Loebsack. Thank you, Mr. Chairman.
1814 I guess this could be one of those things, be careful what
1815 you wish for.
1816 I remember 25, 30 years ago, you know, people thought this
1817 would be great. And it is. It really is. It's Transformational
1818 to our world, but also there some down sides. It's a serious
1819 issue.
1820 And Mr. Zaneis, you point out it's not only about ads, it's
1821 about national security. It's about all kinds of law
1822 enforcement. And so that's why we have to really strike a very
1823 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. Okay.

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 smart phones.

One phone had all the things that was, like, on airplane mode, all the wifi 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 D.C. -- 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 five 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?

Mr. 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.

I think we don't know the -- 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 -- 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. Okay. 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. Okay. 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 five 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?

Mr. 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. Okay. 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, okay, 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, 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.]