CONSUMER WATCHDOG HOLDS A CONFERENCE ON THE FUTURE OF ONLINE CONSUMER PROTECTIONS

DECEMBER 1, 2010

SPEAKERS:
DAVID VLADECK,
DIRECTOR,
BUREAU OF CONSUMER PROTECTION,
FEDERAL TRADE COMMISSION

DEBORAH PEEL,
FOUNDER,
PATIENT PRIVACY RIGHTS

JEFF CHESTER,
CENTER FOR DIGITAL DEMOCRACY

DANIEL WEITZNER,
ASSOCIATE ADMINISTRATOR OF POLICY,
NATIONAL TELECOMMUNICATIONS AND
INFORMATION ADMINISTRATION
DEPARTMENT OF COMMERCE

JAMIE COURT,
PRESIDENT,
CONSUMER WATCHDOG

JOHN SIMPSON,
INTERNET PRIVACY DIRECTOR,
CONSUMER WATCHDOG

SUSAN GRANT,
DIRECTOR OF CONSUMER PROTECTION,
CONSUMER FEDERATION OF AMERICA

GINGER MCCALL,
STAFF COUNSEL,
ELECTRONIC PRIVACY INFORMATION CENTER

CHRIS SOGHOIAN,
GRADUATE FELLOW,
CENTER FOR APPLIED CYBER SECURITY RESEARCH,
INDIANA UNIVERSITY

GARY REBACK,
COUNSEL,
LITIGATION PRACTICE GROUP,
CARR & FERRELL

MELANIE SABO,
ASSISTANT DIRECTOR,
ANTI-COMPETITIVE PRACTICE DIVISION,
FTC

SCOTT CLELAND,
PRESIDENT,
PRECURSOR LLC

STUART BERNSTEIN,
LITERARY AGENT

MICHAEL CAPOBIANCO,
SCIENCE FICTION AND FANTASY WRITERS OF AMERICA

SALLEY SHANNON,
AMERICAN SOCIETY OF JOURNALISTS AND AUTHORS

[*]
COURT: Good morning. Thanks for coming.

I'm Jamie Court. I'm president of Consumer Watchdog, and I'm really glad to welcome you all here for the Future of Online Consumer Protection Conference.

We're not only joined by many great guests in the audience but we're also streaming internationally on the Web, which is great because the weather is preventing probably a few people from getting here. So we're glad you all came.

When we scheduled this conference two weeks ago we didn't realize it would be such a busy day. Today, as many of you know, the Federal Trade Commission is going to be releasing its much anticipated report on online consumer protections and the viability of a "do not track me" list which is, we hope, going to be great news. And we're going to get a preview I understand in a few minutes from our keynote speaker, the FTC consumer protection chief David Vladeck, who's going to be with us.

We also had an action yesterday on antitrust...

(AUDIO GAP)

COURT: ... our European regulators...

(AUDIO GAP)

COURT: But we're not just talking about privacy at this conference. We're going to be talking about antitrust. We're going to be talking about medical privacy, moving beyond the "do not track me" list. We're going to be talking about Wi-spy. We're going to talking about the growth of online power by companies that have in large ways pushed the creative arts and creative artists out of business.

And hopefully we'll be ending around 2:30 today and at the end of the day we'll have some solutions to take forward.

I just -- before I bring out Mr. Vladeck -- I just want to tell you a few things about Consumer Watchdog for those of you who may not know. We started about 20 years ago in California and we opened a small storefront office in 2008 in the capital. Because we really believed there's a lot of hope for change in Washington.

And we did work on health insurance reform, for some greater consumer protection, some other issues, but we really believe privacy now is the greatest hope for...

(AUDIO GAP)

COURT: ... change, and we believe it's because of a...

(AUDIO GAP)

COURT: ... industry who'd spent $60 million to stop the ballot measure. It passed, narrowly, and 20 years later it saved about $62 billion for consumers on their auto insurance bill. And that's from the Consumer Federation of America's report in 2008. It was the greatest reform of the property casualty industry and it was done only because Californians were so angry about their auto insurance rates.

We pioneered patients...

(AUDIO GAP)

COURT: ... laws at the ballot box too because...

(AUDIO GAP)

COURT: ... when 90 percent of Americans believe in something it should happen. It should happen in this country. When a supermajority of people, more than 70 percent of Americans believe in something it should happen.

From the same poll, what percentage of Americans believe that they should have a "make me anonymous button" on the Internet? Make me anonymous -- 86 percent of Americans. This is a real poll. Eight-six percent of Americans believe they should be anonymous on the Internet and yet we don't have this technology. Eighty-four percent believe we should prevent online companies from tracking personal information or Web searches without explicit written approval. Eighty-four percent of Americans.

This is a very popular issue. Popular opinion is with us.

Banning the collection of data for children, 84 percent. Supporting extending current advertising protections against -- about children beyond TV to the Internet, 81 percent. Requiring the creation of a "do not track me" list for online consumer protection -- for online companies that would be administered by the Federal Trade Commission. Eight out of 10 Americans want a "do-not track me" list. When eight out of 10 Americans want something there's a good chance they're going to get it.

And that's why this conference was convened, to come up with solutions like this. So I'd like to -- I'd like to bring up -- before we bring up Mr. Vladeck, point out a few people in the audience who are -- who you're going to see today from Consumer Watchdog who are going to be moderating panels. One is Carmen Balber, who is in the back of the room. She is our Washington, D.C., director. She opened our storefront office a couple of years ago and brought this expose, confront, change plan to Washington, which isn't always easy.

And another man who is going to come up and introduce Mr. Vladeck is John Simpson.

Let me tell you about John. John is our internet privacy director, but John was a journalist for many, many years and before that he was a bit of a hell raiser, and after he got out of journalism he came to us and literally took on the stem cell research industry in California. We had a $3 billion plan for stem cell research and John made sure that when stem cell research grants were given out in California the public got a return on those investments.

He actually busted up with the Public Patent Foundation patents for stem cell research that shouldn't have been given to create more stem cell research. And now he's moving on to other things. He's the director of our Inside Google Project.

So let me bring up John to introduce Mr. Vladeck, and hopefully we'll hear from Mr. Vladeck a little bit about what the FTC's doing today.

John?

(APPLAUSE)

SIMPSON: Thank you, Jamie.

Good morning everyone right here in the room and also who are watching us on the Web. I've got a great pleasure to introduce David Vladeck who as you all know is director of the Federal Trade Commission's Bureau of Consumer Protection. They describe themselves as being the bureau which works to protect consumers from unfair, deceptive or fraudulent practices. The bureau conducts investigations, sues companies and individuals who violate the law, et cetera, et cetera, et cetera, et cetera.

I think of as the guys who get the 144-page complaint that a number of us have recently filed. We're the folks who sometimes make a lot of extra effort for David's office, and we're glad that he gives great attention to those kinds of things.

We did join last week with the Center for Digital Democracy and the World Privacy Forum and USPIRG filing a complaint complaining about deceptive medical practices, and we'll hear more about that later today.

David is on leave from the Georgetown University Law Center. He, before joining Georgetown, had been over 25 years with Public Citizen Litigation Group, which means that he really is a veteran of consumer protection and has seen it from all sides.

So we've asked him to tell us as much as he can about the report that we all know is coming out today. He will also be testifying, I believe, tomorrow before Bobby Rush's committee. I suspect he might be able to say a little bit about that. Washington protocol of course is that he can't say a lot about that. But we do welcome him to offer his views as much as he can on those things, and he's agreed to take questions afterwards. Thank you.

David?

(APPLAUSE)

VLADECK: Thanks. It's sort of like old home week. I think I know at least, you know, three quarters of the audience personally. So it's really wonderful to be here today and I'm grateful for you all coming out in this torrential rain that we're having.
As Jamie mentioned and as John mentioned, today marks an important step forward in the commission's work on privacy. Later today, at 11 am, assuming we get this right, we'll issue a report setting out staff's preliminary recommendations for a new privacy framework.

I will give you a sneak preview of the topics covered by the report at the end of the presentation, largely to keep you captive until then. I know that if I do this at the beginning there will be a huge migration out of here.

So the report will be posted on our website around 11, and at 1 today there will be press availability with the chairman and some of the key staff who authored the report.

For members of the press, if you want to participate, just talk to our press office.

So now we know that there's an elephant in the room. Let me turn to what may be more mundane but are equally important matters, which are enforcement of privacy laws, which is what we spend a lot of our...

(AUDIO GAP)

VLADECK: When Echometrix software is installed on a computer, parents can view the activity taking place on the target computer. That is, they can monitor what their kids are doing online.

Echometrix also advertised a Web-based market research software program that it claimed would allow marketers to see -- here I'm quoting their advertising, "unbiased, unfiltered, anonymous content from social media websites, blogs, forums, chats and message boards."

We alleged that one source of this conduct -- content -- was the online activity of children recorded by parental monitoring software and then collected by Echometrix. We charge in our complaint that

Echometrix failed to adequately disclose to parents that it would collect and share the information it gathered from their children with third-party marketers.

Echometrix made only a vague disclosure about information sharing and placed it about 30 paragraphs into a multi-page, turgid end-user license agreement.

We have talked a lot in the past about the importance of transparency. Burying an ambiguous statement in a EULA just doesn't cut it. That's especially true when the personal information involved is about children.

The consent order requires Echometrix not to use or share information it obtains through its Sentry parental monitoring program, or any similar program for any purpose other than to allow registered users access to his or her account. The order also requires the company to destroy the information it had transferred from Sentry to its marketing database.
I want to acknowledge, and this amplifies a point Jamie and John made, that petitions from the Electronic Privacy Information Center and the Center for Digital Democracy spotlighted these problems with Sentry. We appreciate the input we get and we read all these petitions and take them seriously, even those that are somewhat longer than "War and Peace."

(LAUGHTER)

Better plot though.

Let me turn to data security. This occupies a huge amount of our time. Thus far we've brought 29 data security cases, ranging from cases against retailers, software providers, mortgage companies, data brokers and others.

These cases have involved companies that failed to take reasonable measures to protect against both high-tech hackers -- most recently our case against Twitter -- as well as low-tech dumpster divers.

These cases send a strong message that companies have to take reasonable measures to safeguard consumer data. Companies are stewards of the information they maintain and they've got to be responsible stewards.

To leverage our resources to best effect we're always looking to

partner with law enforcers both in the United States, and as I will talk about in a few minutes, with our partner overseas.

For example, the commission just finalized our most recent data security case against Rite Aid pharmacy and drug store chain. We coordinated our investigation with the Department of Health and Human Services, which was looking into Rite Aid's handling of health information under HIPAA. We alleged that Rite Aid failed to implement reasonable measures for handling personal information about customers and job applicants, particularly with respect to its disposal practices.

Our action followed media reports that Rite Aid pharmacies across the country, and I'm not making this up, were throwing pharmacy labels and employment applications into open dumpsters.

By cooperating with HHS we were able to get broad relief. Their order covered Rite Aid's pharmacy practices regarding prescription information. Our order required security for the front part of the store and for employee information.

Although we do not have authority to get civil penalties in these kinds of cases, HHS was able to get a very substantial civil penalty against the company.

We've reached similar agreements the prior year with CVS Caremark relating to their conduct, again working with HHS to coordinate our efforts and the scope of relief.
We also cooperate closely with the states. For example earlier this year we settled a case against LifeLock. Our case was brought simultaneously with cases by 36 states attorneys general in one of the largest federal-state cooperation...

(AUDIO GAP)

VLADECK: ... efforts on privacy ever...

(AUDIO GAP)

VLADECK: ... existence of God.

During the middle of our settlement talks the CEO himself was victim of identity theft. The settlement bars deceptive claims, requires data security measures and compelled LifeLock to pay $1 million to the states and $11 million for consumer redress. I'm happy to announce that this week we mailed out redress checks to nearly a

million customers across the country.

Our data security work is important, but I'm equally excited about the work we've been doing to make businesses respect consumer choice. The statistics that were cited earlier today simply confirm, I think, what we all know. Consumers want control over their personal data and they want to be able to ensure it is adequately safeguarded.

There are cases that we bring because we don't think those safeguards have been implemented appropriately. One case is Echometrix, which I just talked about. Another is our recent action against an online data broker, U.S. Search, that charged consumers $10 to opt out from its database but did not always opt them out.

U.S. Search sells public record data information, such as names, addresses, phone numbers, marriages and divorces, bankruptcies, associates, criminal records, home values -- you know these services.

So you could order up a search like people search, background check, real estate reports, criminal records, court records, those kinds of things, and return the name of an individual associated with those actions. U.S. Search promised that it could lock consumers' records so others could not see them, but as we alleged in the complaint consumer information still showed up in many instances, even after consumers paid their fee.

For example, if I opted out as David Vladeck some of that information might not come up. But information that used my middle name or some variant of my name would certainly remain in the database and be generally accessible.

The settlement prohibits misrepresentations about the effectiveness of any service that purports to remove information about consumers from the website and requires U.S. Search to give full refunds to the nearly 5,000 customers that it had signed up.

Those who think that people don't care about privacy might be surprised to learn that 5,000 people found this site and were willing to pay to ensure that their information was kept private.

So the message here is that when consumers choose to take advantage of a company's opt out mechanism the company must implement that choice effectively. And of course that's true whether or not the consumer has paid for it.

Our investigations do not necessarily result in the filing of a

complaint or a settlement. Let me give you two quick examples.

Last summer I sent a letter to individual stakeholders in XY Corporation (ph) which operated a now defunct magazine and website directed to gay youth, male gay youth. The letter expressed concern about these individuals' efforts to obtain and use old subscriber lists and other highly sensitive information, including names, street addresses, personal photos and bank account information from gay teens.

The letter warned that selling, transferring or using this information would be inconsistent with the privacy promises that were previously made to subscribers and may violate the FTC Act. Thus the letter urged that the data be destroyed.

After receiving a copy of our letter the court overseeing the bankruptcy proceedings involving XY Corporation (ph) ordered the destruction of the information.

Also, at the end of October, we closed our investigation into whether Google's collection of unsecured Wi-Fi transmissions was deceptive or unfair in violation of Section 5 of the FTC Act.

Google's information collection was the subject of a petition by Consumer Watchdog. There's been a lot of discussion about our closing letter in that matter. Most of it I would say certainly uncharitable to the Federal Trade Commission.

Here is what I think you should...

(LAUGHTER)

... here's what I think you should know about it: First, Google's conduct involved the unconsented to...

(AUDIO GAP)

VLADECK: ... be reasonably expected to cause significant harm to consumers. In this case there is no evidence of harm that would satisfy that test.

Third, we took steps to ensure that there would be no recurrence of this episode by Google.

At our urging Google implemented a number of measures to prevent privacy violations in the future. Many of these measures build

privacy into product development and ensure that Google engineers and managers receive core privacy training. These measures are summarized in a letter I sent to Google on October 27th, 2010, which is available on our website.

(AUDIO GAP)

VLADECK: Fourth...

(AUDIO GAP)

VLADECK: ... perhaps it wasn't sufficiently clear in our letter, but that's why we did what we did.

In addition to investigations involving companies, individual companies, we're also engaged in broader privacy initiatives. We're viewing our Children's Online Privacy Protection Act rule to see whether it provides adequate protection in light of significant changes in the marketplace affecting kids such as the explosive growth and use of social network and smart phones and the development of technology such as interactive TVs.

Our rule review is about how will this statue, which is just ironically 12 years old, has stood the test of time. For example this (inaudible) coverage of websites located on the Internet and online services reach the kind of electronic media kids use today.

How should we address the collection of mobile geo-location data? Or information collected in connection with online behavioral advertising? What about online gaming sites that appeal to children. Should they be covered? And are the methods for verifying parental consent, such as using print and sent forms, outdated or obsolete?

We are also looking for creative ways to encourage compliance with consumer protection laws. Let me talk about a couple of these initiatives.

One of these concerns history sniffing. I always think of sort of a Saint Bernard sort of coming up to me. But researchers at the University of California at San Diego released a paper recently demonstrating that 46 websites were using a sniffing practice to learn about consumers' web history without their consent.

History sniffing allows websites to surreptitiously collect private information regarding a consumer's Web browser without installing cookies or using hacking tools and without any action on

the consumer's part.

This is invisible to the consumer and this technique deliberately bypasses the most widely known methods consumers use to prevent online tracking, which is deleting cookies.

Companies can do this by exploiting a feature of consumers' web browsers that displays hyper links in different styles depending on whether the consumer has previously visited the website associated with the link.

When a consumer navigates to a website that contains history-sniffing code, the code can check whether the consumer has visited a list of dozens or hundreds or even thousands of sites.
In theory, history sniffing could be used to get extensive information regarding the domains or even subdomains the consumer had visited. For example, the USS -- the UCSD researchers found if a consumer visited a certain gaming site, for example, Web-sniffing codes would then check whether the computer...

(AUDIO GAP)

VLADECK: ... had visited, for example...

(AUDIO GAP)

VLADECK: ... to take care of this problem. A couple of browser companies have already rolled out fixes and we've been told that the others are implementing fixes now. So consumers who upgrade to the latest version of their browsers will no longer experience this vulnerability.

We're on the lookout for similar tactics that companies can use to extract consumer information by technical means without the consumer's knowledge.

OK, so now -- so now that I've -- I've -- you've indulged me for long enough, let me turn to the subject you've been waiting for...

(AUDIO GAP)

VLADECK: ... which are re-examine of the...

(AUDIO GAP)

VLADECK: ... and there have been important innovations. But

self-regulation has not kept pace with technology, and consumers face a daunting burden in today's marketplace to safeguard their privacy.

Take mobile devices. It simply isn't realistic to expect consumers to scroll through privacy policies on today's smart phones. We've seen privacy policies that on a smart phone take 152 pages. It's just -- it's just not -- it's just not possible. And in the 21st century marketplace with the ubiquitous collection, use and storage of data, it's increasingly difficult to identify or pinpoint the harms associated with misuse of data.

Over the last year we've hosted three major roundtables to get public input as part of this privacy reexamination and it looks like half of the people in this room participated in those roundtables in one way or another and we're grateful for that.

So our report will be coming out later today. Let me preview some of the big picture issues without giving away too many of the details. After all my chairman is going to be announcing this at 1 o'clock and I tell you too much at my own hazard.

So let me talk about some of the major themes.

One major theme is that we need to reduce the burden on consumers. Consumers now bear the burden of trying to control their own private information, and that burden is a daunting one to meet.

So one -- one proposal, which builds on existing proposals, is to build privacy into products and services at the outset; that is privacy by design.

There's tremendous value in building privacy and security into companies procedures, systems and technologies by design. This means thinking about ways to practice good data hygiene from the very beginning, such as providing reasonable security for consumer data, limiting collection and retention to the least amount necessary, and implementing reasonable procedures to promote data accuracy.

The more companies do to establish good practices by default on the front end the less burden on consumers to spend lots of time to salvage some privacy at the back end.

Another way to reduce the burden on consumers is to greatly simplify consumer choice. We heard a lot about the roundtables -- at the roundtables -- about streamlining choices for consumers so choice -- so consumers can focus on the choices that really matter to them.

Uses of their data that they would not expect. The way to make privacy choices meaningful to consumers is to present them in a short, concise manner at the point when the consumer is providing the data so data -- so that data and privacy are on the top of the consumer's mind and access to choice is easy and available to them at that moment.

We're also thinking about whether it would be helpful to have more consistent privacy policies so consumers can compare competitors' privacy policies at a glance.

What we're hoping to do is to actually encourage competition on matters of privacy, and the best way to do that is to have comparable privacy policies. I know we'll have made progress when Consumer Reports does an issue that compares competing privacy policies and recommends products in part based on privacy safeguards.

We're also thinking about -- and this is an issue that's discussed extensively in the report -- about strong protections for sensitive information. Health, financial, children's and geo-location data should be a given, but there are questions about what other areas should be treated as sensitive information.

It goes without saying that consumer choices once exercised must be respected. Yet we've seen less reputable marketers abuse technologies in a variety of ways to circumvent consumers' clearly expressed preferences for privacy.

We will not tolerate a technological arms race aimed at subverting privacy-enhancing technologies that consumers have chosen to enable and the report addresses how we will go about seeking that end.

We also need to increase transparency. The report discusses ways to increase transparency about commercial data practices.

(AUDIO GAP)

VLADECK: ... one question...

(AUDIO GAP)

VLADECK: ... storehouses of data about consumers from myriad sources. Some panelists suggested that consumer should get access to their data as a means of improving transparency, others discussed the costs of providing access and recommended that any access should vary

with the sensitivity of the data and its intended use.

Access is an important ingredient in accountability. The report discusses this issue in great depth.

We're also continuing to focus on consumer and business education. We think that this is an integral issue. The report, by Chris Huffnagel (ph) and Joe Thoreau (ph) at the beginning of -- I guess at the end of last year -- underscored the degree of consumer uncertainty and confusion about what happens, what happens in terms of their data, what happens with tracking. I think collectively we need to do a better job educating consumers.

We have tried to put out a lot of guidance. For example, we did a massive surf on data that was inadvertently shared through P2P file-sharing programs. We've done a lot of business education on that issue.

But we all recognize that we need to broaden and deepen consumers' understanding of information collecting, sharing practices so they can take whatever steps they want to take to preserve their privacy.

Recognizing that consumers want control and the ability to go online without being tracked, the report also addresses the viability of some universal mechanism, a one-stop shop where consumers can register a preference not to be tracked or not to be targeted for online ads and where marketers would have to respect consumer choice.

There have already been efforts to allow, by browsers and other providers, consumers to indicate that they don't want to be tracked or to adjust or tweak how they're tracked. These efforts are laudable, but it's hard to say how consumers will respond if many different associations, companies and groups offer different options in different formats.

We have to simplify consumer choice and a "do not track" option can achieve that goal.

Tomorrow I'll testify before a House hearing on "do not track" and provide more details about the commission's position on this issue. But this is an issue that will also be addressed in depth at the report issued 11 and I think that once you read that there will be no secret about the commission's position on "do not track."

So I want you to -- ask you to do one thing today which is to

read our report, let us know what you think...
(AUDIO GAP)

VLADECK: ... particularly this community. We need to hear from you. We need to know what you think, and we're thick skinned so if we haven't gotten it right please let us know.

So I promised John I'd leave some time for questions.

SIMPSON: Well, thank you, first of all for coming.

(APPLAUSE)

We have a mike that's going to go around so if anyone wants a question they need to raise their hand and ask Josh for the mike. There's one over there from Susan Grant.

But let me, Mr. Vladeck, while we're doing that, just one quick question. I know it's not 11 but the industry says that a "do not track" mechanism is not viable. Can you tell us basically whether you, in your report and in your findings, find that it is viable for the government to do this and would it take congressional action or is it something that can be done without it?

VLADECK: Well, OK, there's two questions there. Let me separate them out.

In terms of viability I assume you're talking about technological viability.

SIMPSON: Yes, without reducing commercial choices in any meaningful way.

VLADECK: We believe there are technological means to implement a "do not track" system. I don't think there are serious arguments about the technical viability. There have been some concerns about enforceability. We believe that there are ways to enforce "do not track" should it be implemented. We've asked questions about those issues, but of course that presupposes that we're going to take a particular position on "do not track" which of course I'm agnostic on at least until 11 am.

(LAUGHTER)

SIMPSON: And should you have a position would it be that Congress would have to pass legislation to get it up and running or

could it be something that could be done on a stand-alone basis?

VLADECK: Well again that's a complicated question for this reason. I do not think that under the FTC's existing authority we could mandate unilaterally a system of do not track. We've never claimed that authority and I think that it would be hard to cobble together a winning argument based on our authority that we could essentially tomorrow issue an edict requiring do not track.

There are ways that we can coax, cajole and charm industry in that direction, but I think that -- and I don't think this is controversial -- I think that if the decision were made by Congress that a do not track system ought to be put in place and put in place immediately, it would take an act of Congress not an act of the Federal Trade Commission.

SIMPSON: Susan, sorry.

GRANT: Hi, good morning. Susan Grant, Consumer Federation of America.

First, I just want to thank you for your leadership at the FTC and your strong commitment to protecting consumers' privacy.

But as you know Consumer Federation of America and others have objected to the U.S. Search agreement because it neglected to take up an issue that we think is at least as important as disclosure and that's the central issue of whether a company like that should be able to charge consumers for not selling their information.

Does the FTC need broader authority in order to address issues like that?

VLADECK: That's a fair question that I would need to think longer and harder about before I give you an off the cuff answer. I think there are reasons why we didn't push that issue in this case but I'm not sure those issues were tied up in questions about our authority.

So that's a fair question and I will give you an answer but I'm not going to give you an answer right now.

SIMPSON: Any questions on this side of the room, reporters, anyone who's got something?

VLADECK: Am I going to get out of here?

SIMPSON: No. We've got a few questions.

Jeff, you had something? Jeff Chester.

QUESTION: The crazed -- I'm the crazed mini-Tolstoy. In what way is the FTC working with FDA to help the FDA...

(AUDIO GAP)

QUESTION: ... what relationship is there between -- is there a relationship between the FTC and the FDA and HHS on these issues so there can be a more coherent focus? Thank you.

VLADECK: Yeah, this is again a question I have to be somewhat delicate about because we do have very close ties to the Food and Drug Administration. It is one of the agencies with which we have enormous overlapping jurisdiction.

We have jurisdiction over, really, the marketing of any product including drugs, medical devices, dietary supplements, foods. They have jurisdiction, too, over labeling, which is construed broadly by the courts to include essentially advertising.

Historically, the FDA's principal focus has been on labeling and on direct-to-consumer marketing generally through the deployment of 90,000 or 100,000 detail men who work for pharmaceutical and device companies who visit health care providers -- doctors, hospitals, and so forth -- and sell face to face.

I think it's fair to say that the FDA's experience with other forms of marketing, particularly the kind of marketing your petition focuses on, is far less substantial than ours. And so we have as part of an ongoing relationship we've had with the FDA, we've lent our expertise and we talk to them about these issues.

And so we are hoping, moving forward, to deepen our ties to the FDA. Recently we have done a fair number of public actions with the FDA. Two weeks ago we jointly sent warning letters to the manufacturers of highly caffeinated alcohol beverages that were being marketed principally to young people. This was a joint effort. We had been investigating some of these companies for quite some time, as had the FDA.

We sent out warning letters on all sorts of things, the use of dietary supplements -- DHA, which is a dietary supplement that some

argue promotes brain development. DHA was being widely used to market children's vitamins based on claims that we didn't believe that were accurate. We sent out a raft of warning letters to companies engaged in that practice.

So there's a long solid history of collaboration between the Food -- the Food and Drug Administration and the Federal Trade Commission and...

(AUDIO GAP)

QUESTION: ... government agencies that have pledged to continue using Internet Explorer 6 for the next few years because they believe that the cost of upgrading their internal applications and their computer systems is too great. And so we are going to have millions of consumers who are not protected.

What is the FTC going to do about this and what should those consumers do? Because either they don't know how to upgrade their browser or because they're not in control of their computer and thus not able to upgrade it themselves.

VLADECK: That's a great question. I think there are things that we're doing that are both public and non-public. Let me start with the public ones.

We will be putting out public information on this issue and urge people who have old browsers to upgrade them. And we will give, as we do, what we're hoping is an easy to follow comprehensible advice about how one could upgrade browsers.

There are other actions that we're taking here that I can't talk about. But this is a matter that we do want to publicize to encourage people to upgrade their browsers to avoid inadvertently having their history sniffed when they visit a website.

SIMPSON: Could we take a couple more questions?

QUESTION: Just wondering how much in the report is just recommendations and how much can you actually implement and mandate.

VLADECK: That's, too, a good question. I mean, the report was intended to provide a vision, a privacy framework moving forward, recognizing that given the commission's jurisdiction we couldn't mandate all of it. And this is an issue that the report is candid about and addresses.

But I would say some of it we can implement on our own, some of it we can't, and if you wanna read the report and then ask me that question I may be able to give you a more intelligible answer.

SIMPSON: Can we -- before you ask questions can you please identify yourselves, your affiliation and your name? This is being broadcast and that would be most helpful.

Is there any reporter questions, just before we get to -- just so we can get this (inaudible) any more reporter questions?

OK, Josh do you want to go here and there.

One quick question while (inaudible) the mike. State-based measures, state ballot measures to deal with some of these issues. Do you think there is -- is that a problem from your point of view for preemption? For instance if there was a do not track me mechanism created through a ballot measure process in the state of California. Do you see any obvious barriers to that?

VLADECK: Well, obviously I'm speaking for myself and not the commission, but I think it is fair to say that particularly on these issues the commission has always seen what it does as a floor not as a ceiling. So state (inaudible) notification laws.

California has laws prescribing -- requiring some form of privacy policy.

We've never taken the position that state action is preempted based simply on the existence of an FTC mandate of some kind. And while I can't bind the commission on this, the commission's position has generally been to encourage state enforcement and to encourage state action in these areas.

(AUDIO GAP)

QUESTION: ... very broad definition of surveillance, observing, watching, following, and many times people (inaudible) and say, "I don't track. I do analysis. "

VLADECK: Well, I think we're talking about any collection of consumer information which they do not consent to. I don't know whether that meets your definition, but I think that's what we're talking about when we're talking about tracking.
QUESTION: Charlie Leocha from the Consumer Travel Alliance.

I have been involved with, at lower levels in the FTC, of trying to get airline computer reservation systems and general global distribution systems kind of at least looked at by the FTC. I just wanted to ask you, has that bubbled up to your level yet?

VLADECK: I think it has bubbled up to the Office of General Counsel's level, which I don't control. I mean, There is a jurisdictional question that I think needs to be resolved and that' -- that's -- you know, there's another part of the agency that is responsible for doing that.

QUESTION: OK. Then that kind of answers the second part of my question, so I'll ask you that privately later.

VLADECK: OK.

SIMPSON: OK. We got maybe one more, two more.

(CROSSTALK)

QUESTION: Hi, this is Ellen Blackler at AT&T, and I'm going to ask the important question on December 1, which is when are comments due on this report?

VLADECK: Well, there is a question I can answer. Comments will be due on January 31st, which is a Monday. So we're -- we want to move this along but we recognize there are holidays and so forth. And we've tried to -- as you'll see in the report we've tried to make this easier for commenters because we are quite specific in the questions we've asked. This is no longer a question about why is there air, 300 words or less. I mean, we've tried to be quite directive about the kind of information that we're asking for.

QUESTION: This is Ivanna Ruse (ph) from Consumers Union. My question was about anonymization and to the extent that you can talk about this. I know a lot of entities are saying, you know, "We don't track personally identifiable information. We only have a unique identifier or an I.P. address. So no harm no foul. There's no problem there. We're not violating anyone's privacy."

So maybe to the extent that you can talk about what is the FTC's position on this?

VLADECK: That's an easy one because we resolved that last February. Our position has been since we issued our "Online

Behavioral Advertising" report in February 2009 is we don't accept that argument. That is, we understand how -- unfortunately -- how easy it is now to link things like an I.P. address with more about individual consumers. And we all know that there are...

(AUDIO GAP)

(CROSSTALK)
VLADECK: We have no jurisdiction over wiretapping. There are at least two other federal agencies that do. One has publicly announced that it is engaged in an investigation, and on that I will say no more.

SIMPSON: Thank you so much.

VLADECK: OK, well, thanks, John.

(APPLAUSE)

SIMPSON: We're going to bring up our first panel just to stay on time. Susan Grant from the Consumer Federation of America, Chris Soghoian, and Ginger McCall from EPIC. And we'll get going right away.

So we're just going to keep on going through if we can get the mikes on because we're broadcasting and we want to keep on time for you guys. There's some coffee in the back and we'll do a break after the next panel.

So we're going to take a few minutes just to get some comments, maybe five minutes or seven minutes or so from each of the panelists about what they heard...

(AUDIO GAP)

SIMPSON: from Mr. Vladeck (inaudible) from the Consumer Federation of America, who is the director of Consumer Protection. And she is also, as I understand it, going to be testifying tomorrow on the do not track me list at the House -- the House Energy and Commerce Committee hearing.

She has been doing these issues for a long, long time and works specifically in the area of privacy, deceptive marketing, online safety, security, fraud, electronic and mobile commerce, and general consumer protection issues, and she coordinates the CFA's Fake Check Task Force which conducts the Consumer Federation of America's Annual

Consumer Complaint Survey.

And she began her career in 1976 at the Consumer Protection Division in the Northwestern Massachusetts District Attorney's Office. So she's been watching these issues for a long time and has very a keen eye. So we'd like to welcome Susan.

GRANT: Thank you very much.

Well, I think I heard good things about do not track from David Vladeck, but I'll have to read the report to make sure.

Just an overview of the issue. Consumers are being tracked on the Internet wherever they go, whatever they do, without their knowledge and consent. Information about their online activities, what they search for, what they click on, what they purchase, even who their friends are in social networking sites are being compiled and analyzed and used to profile them.
This behavioral tracking is primarily used at this point to deliver ads tailored to consumers' inferred interests, but it can also be used to make assumptions about people for things such as employment, health insurance and financial services.

There are no limits to what types of information can be collected, how long it can be retained, with whom it can be shared and how it can be used. Consumers simply have no legal control over being...

(AUDIO GAP)

GRANT: ... spied on when they go online. (inaudible) that information collected in this manner can be used for purposes of lawsuits and government surveillance.

Voluntary industry programs simply aren't adequate to give consumers the control they need. They're full of loopholes.

For instance, some define sensitive information very narrowly as just health records, and so a lot of activities that consumers might engage in online that are health related wouldn't be covered by those voluntary standards. And they also make exceptions, usually for sharing among affiliated companies, not giving any consumer control in those situations.

Not all companies participate and there are no real penalties for failure to comply. Plus, some of the programs rely on placing cookies

on consumers' computers, which are not always effective in stopping different kinds of behavioral tracking and are not necessarily persistent over time.

The Federal Trade Commission decided in 2003 that it was too burdensome for consumers to have to opt out of telemarketing calls company by company and that the voluntary programs, such as the Direct Marketing Association's Telephone Preference Service, just weren't adequate to protect consumers for precisely the reasons that I described. And that was why the FTC created the immensely popular do not call registry.

The same rationale now applies to online behavioral tracking and calls for the need to create some sort of do not track mechanism for consumers who do want to avoid cyber-stalking.

I know that Chris will talk about what this would look like in terms of the technicalities, but as we envision it, this would not be something like the do not track -- do not call registry that consumers would have to sign up for and provide personal information. Rather, it would be a browser-based solution that would be simple for both consumers and trackers to use.

All browsers in our vision would be required to have a do not track mechanism as a standard feature at no extra charge to consumers and all companies would be required to honor their privacy preferences.
The FTC, in our view, would play a very important role by doing mystery browsing and taking other measures to ensure in fact that companies were complying with do not track since it's very difficult for consumers to detect whether they're being tracked or not. And we think that consumers should also have the ability to enforce their legal rights.

There is a fact sheet in your packets about why we need a do not track mechanism. And I'm anxious to see the FTC report to see if it gives strong support to this notion. I hope that it does.

Thank you.

SIMPSON: Thank you, Susan. Thanks.

We are -- we're going to go to Chris Soghoian now, who is a graduate fellow at the Center for Applied Cyber Security Research at Indiana University, and his research has focused on the intersection of applied computer security privacy law and policy.

His work has resulted in a lot of successful passage of amendments in Indiana's data brief breach law and congressional investigation of security flaws in the Transportation Securities (sic) Administration. And my favorite was he found a persistent cookie by Google very early on against the White House's own privacy policies on one of the first days the White House got its website up and got him to take it down.

So he is a sleuth, a super cyber-sleuth who has been in a lot of media storms and he, in 2009, he had disclosure of evidence revealing Sprint Nextel had provided its customers with GPS information -- their customers' GPS information to law enforcement officials over 8 million times in a single year.

So he is a guy who goes online and finds things and understands how Internet companies track us, which is why he understands and I hope will address the technology that's needed and is able to stop that type of tracking and what its requirements would be.

Chris?

SOGHOIAN: Thanks.

So I've been playing in the space for a little while, and I'm probably one of -- I have a very unique role in that I'm both an activist, a researcher -- until a few months ago I worked with the Federal Trade Commission, I was there for the last year as their first ever technologist. And so I have seen things on both sides.

Before I sort of get into the do not track mechanism I'd like -- one of the proposed mechanisms -- I'd like to talk about how we got here and why we need to move to something like this.

So the web browser is the primary privacy enhancing technology for consumers. Right? Most consumers do not have software that they bought at Staples. In fact, it's very difficult to find privacy software on the shelves of stores. And so they trust the web browser to protect them online.

(AUDIO GAP)

SOGHOIAN: ... with the expectation that it'll protect their privacy. But many of them don't realize that the web browsers they use are made by ad companies. Right? So Microsoft Internet Explorer, Microsoft has an ad network. Google's Chrome. Google has an ad

network. Mozilla Firefox. Most of their budget comes from Google for a search deal. And similarly Apple is both an ad network now and they get a huge pile of money from Google for having the search engine be the default.

And so all of the browser vendors are in one way or another either directly supported by ad networks or are themselves ad networks. And as the Wall Street Journal has spectacularly demonstrated both with an expose into Microsoft by (inaudible) and yesterday into Mozilla, oftentimes the browser vendors' motivations into the features they include in their software and the defaults that set these features, the design decisions are motivated or influenced by a desire to not hurt their own advertising divisions.

And so it's not surprising for example that the in private filtering mode in Internet Explorer needs to be turned on each time you use your browser. It's the only feature in the browser I'm aware of where you have to reset it each...

(AUDIO GAP)

SOGHOIAN: ... said that he would like to see these companies competing on privacy, but right now the browser vendors are not competing on privacy.

So I've been looking into cookies and tracking for a while and, to be frank, the situation right now is laughable in terms of the ease with which consumers can try and protect themselves or the difficulty in which they can do it. There are more than a hundred different opt-outs from different ad networks around the world. Some ad networks are members of the Network Advertising Initiative. Some of these cookies are located on one website.

There's now going to be a new industry website that's going to have other opt-out cookies. But there certainly still isn't a single one-stop shop.

Even if there were a one-stop shop where consumers could obtain all of the opt-out cookies, we have the problem that we're using cookies, which are something that can be deleted. In fact we recommend to consumers that as a privacy-protecting feature they delete cookies. All of the browser's private browsing modes delete cookies when you close the private browsing mode. Right?

And so we have this situation where the tool that you use to say no to tracking is one that can be erased. In fact we encourage people

to erase it. It's very difficult for consumers to tell the good cookies from the bad cookies, to tell the online shopping cart cookie or the "please recognize me the next time I sign in" Amazon cookie to the stealthy cookie used by DoubleClick or Atlas or one of these other ad networks.

You know, last year I published a survey of behavioral advertising network opt out cookies and showed that even if the consumer didn't delete the cookie themselves many ad networks had intentionally set their opt out cookies to be six months or less. Right?

So that means even under ideal circumstances consumers still had to go back to the advertiser's website every six months to get new opt out cookies.

Clearly this mechanism wasn't working. And so last year I built a tool for browsers called TACO (ph) that collected all of the opt outs into one place. This saw some adoption, but still this is a third party tool that very few people were using.

Since then some other groups, including the NAI, have built their own plug-ins. And so there's probably four or five different opt out plug-ins that consumers can use today to try and opt out of the networks.

There are two issues here though. The first is that, as David said, there's a difference between do not track and do not use. And all of the ad networks -- or most of the ad networks right now only let consumers opt out of the use of their data. Even if you opt, out the ad networks continue to track you around the web.

The other issue is that because of the way web browsers work right now, when you install a third party add-on you're giving it administrative access to your browser.

And so I think there's something particularly perverse about having to give a software tool created by an ad industry collaboration administrative access on my computer so that they won't track me online.

And so until the web browser renderers build something into their products by default, I think the plug-in mechanism just isn't going to work.

And so to bring this to sort of the do not...

(AUDIO GAP)

SOGHOIAN: ... love to have something in their product. But they didn't want to be in the business of updating a list of cookies and they didn't want to have to roll out an update to consumers each time a new ad network came on the horizon. They wanted to have a single check box that consumers could use. And the browser didn't want to be in the business of keeping something up to date -- a list of opt-out cookies.

And so it was because of that that people started thinking about the idea of an opt-out header. The proposal that is now on the table -- you can see -- there's a website that two guys at Stanford have put together -- it's called www.donottrack.us. It describes a lightweight technical mechanism.

The short version of it is that your browser would send a signal to every site you interact with that basically says, "Leave me alone." It would be a single check box in the browser and then the ad networks would receive that proactively. The ad networks wouldn't have to do anything to receive it, they would just have to look for it. And then the question we're then left with is what do the ad networks do once they receive it.

I think do not track means do not track. I think it means that they should not track consumers, they should not give the consumers any cookies, they should not log any data, they should not try and fingerprint users, they should not abuse browser flaws to dig through their browsing history. It should mean do not track.

But my fear is that industry may try and weasel this one and -- and -- and just say that do not track means do not use. That really what we're talking about is shifting from a cookie-based opt-out mechanism to a browser-based opt-out mechanism. But I think the ad networks will continue to want to track users even when they opt out because that data is really valuable and they can always sell it to someone else.

So there are some technical proposals on the table. It would not be difficult to get the browser vendors to build it in. The difficult thing is going to be to get the ad networks to agree to support it, and I think that's where the FTC is going to need to play hardball.

And if the FTC doesn't have authority I think Congress is going to need to give them that authority, but I don't think the ad networks

are going to voluntarily agree to support any kind of strong mechanism unless their arms are twisted.

Thank you.

(APPLAUSE)

SIMPSON: Thanks, Chris.

Now we're going to change the discussion just a little bit before we go to a back and forth with Ginger McCall who is the staff counsel assistant director at EPIC, and EPIC's Open Government Project. And she works on a variety of issues at EPIC, including consumer protection, open government requests, amicus briefs. She litigates EPIC's Freedom of Information Act lawsuits and is the co-editor of litigation under the federal government laws...

(AUDIO GAP)

SIMPSON: ... 2010. And she's authored several ...

(AUDIO GAP)

MCCALL: ... of the do not call list, it was by a congressional mandate. There was the Telephone Consumer Protection Act, which directed the FCC to initiate rulemaking concerning the need to protect people's privacy rights and allow them to avoid phone solicitations.

So that allowed the FCC to then seek comment from the public, which EPIC submitted comments, EPIC and numerous other organizations. And what we wanted initially was something that was based on an opt-in model as opposed to an opt-out model, because we felt that that was more faithful to privacy protection and to privacy laws.

Unfortunately the FCC did end up going with an opt-out model, but on the whole the do not call list worked out pretty well. On its first day, in fact, 10 million people registered for that list.

There were of course legal challenges, which I think probably we have here if there was some sort of do not track list. The industry did not go quietly. They challenged it on the basis of the First...

(AUDIO GAP)

MCCALL: ... fees that cover the cost of that list.

I'm going to switch over now to talk a little bit about Street View, which is something that David Vladeck discussed.

When Google started Street View, which was this program to overlay on their Google Maps tool to take a van and drive around and take pictures of streets so that you could see a 3D view of that...

(AUDIO GAP)

MCCALL: ... there was a lot of initial...

(AUDIO GAP)

MCCALL: ... pushed back on this and ended up instituting this program anyway. About a year into the program they instituted certain privacy protections, including blurring out people's faces, blurring out license plates.

But what Google didn't tell people is that aside from the fact that it was collecting images, which were already troubling to many, it was also collecting Wi-Fi data and collecting payload data.

Now, the Wi-Fi data that it was collecting was information about wireless hubs or hot spots. The payload data, which is even more troubling, includes passwords, e-mails, anything that was exchanged over those unsecured Wi-Fi networks in the time that that van was passing by.

And this was not disclosed in any way to the public. In fact it only became public information after it was discovered by European privacy officials.

And Google had been doing this at that point for years. So EPIC was obviously very troubled by this, and we decided that we would file a complaint.

There's really dual jurisdiction over this. The complaint could have been filed with the FCC or the FTC. We decided to go with the FCC for several reasons.

First, the legal reason. The FCC does in fact have jurisdiction over this. But, second, for practical reasons.

We have filed many, many complaints with the FTC and we have seen many of them go unnoticed by the FTC. We have filed complaints regarding Facebook, we have filed complaints regarding online tracking

and marketing, we have filed complaints regarding Google in the past, and the FTC has been slow to act often and often never acting at all.

So we ended up filing our letter with the FCC, which the letter is actually included in the packet here. And in that complaint we cited violations of U.S. law including the Wiretap Act. Which the Wiretap Act provides civil liability and criminal penalty against any person who, quote, "intentionally intercepts, endeavors to intercept or procures any other person to intercept or endeavor to intercept any electronic communication except as provided in the statute."

And so we cited this when we wrote our letter to the FCC. It's surprising, it was surprising to us and it continues to be surprising to us that the FTC has looked at this, they've considered the law, and they've decided that this in fact does not violate the law and decided to drop their investigation.

It seems clearly on its face unfair and deceptive for Google to be sending this van around telling people that the van is collecting images, never disclosing to them that the van is actually collecting information about Wi-Fi and payload data, which includes people's e-mail...

(AUDIO GAP)

GRANT: ... or any activities that they had.

(AUDIO GAP

SIMPSON: Is there something in this culture of these companies? You know, Chris mentions advertising being a key here. You know, Google makes 90 percent of its revenue from advertising. Facebook is going to be making similar amounts from advertising. These are advertising companies. Their culture is driven by engineers and advertising ethos.

How can companies that really depend on advertising dollars -- will a do not track me list be sufficient to stop them. And what are the limits of the list and what are the potentials for the list?

SOGHOIAN: So let me clarify here. No one is talking about a do not track list. People are talking about a do not track mechanism. The reason you hear the words do not track list is because the do not call list is so popular that everyone wants to associate the do not track mechanism with the do not call list.

There would be no -- there would be no government registry of tracking websites. There would be no government registry of consumers who don't want to be tracked. For strong privacy reasons you do not want consumers to go to a website and get a unique identifier just to say that they don't want to be tracked. You want a generic opt out that is persistent and tells people, "Leave me alone."

You also, if I might add, the FTC's enforcement hook is based on unfairness and deception, and unfairness is really, really to show, you have to show harm. And so oftentimes they use deception as a hook because you just have to show the company lied.

If consumers send a strong signal to an ad network, if the consumer says, "leave me alone" and the ad network continues to track you, there may be the possibility of a deception hook there.

If we simply continue the arms race that we've had for the last few years of consumers receive pop-ups, then the web browsers build pop-up blockers, then the ad network evade the pop-up blockers. Web browsers build private browsing modes, then ad networks exploit browser flaws to still track consumers even when they're using private browsing mode.

If we just continue that arms race we don't get any relief, because it's not illegal to engage in a cat and mouse game and innovate around browser privacy controls.

So while I do think the web browser vendors could do a lot to lock down their products and use sane, sensible defaults, I still like the idea of the consumer sending their preference every time they interact with an ad network because that then gives the FTC a hook to go and nail these companies for telling consumers they will obey their preferences and then not doing so.

SIMPSON: So it's more like a do not track me browser or browser plug-in or mechanism that the government would then say these are the specs and this is...

SOGHOIAN: So, you know, the Rush bill included a safe harbor. I could envision a safe harbor in which ad networks that agreed abide by a do not track mechanism would get some kind of protection, and then that way the FTC could go and nail them for opting into the safe harbor and then ignoring the browser's signal.

But one thing with a plug-in: We already know that consumers don't use plug-ins. Even the most widely used plug-in, Adblock Plus,

which I think has 10 million daily users, that's a drop in the bucket to the 400 million daily users of Firefox.

If we're going to have this in the hands of consumers it has to be built into the browser by default. That doesn't mean it needs to be turned on by default, but it needs to ship with the browser by default.

And so part of this, not only do we need to get the ad networks to the table to agree to recognize and obey this thing, but we also need the browser vendors to sit down and agree to build this thing into their products.

SIMPSON: (inaudible) design -- the privacy by design that Vladeck was talking about.

Susan, did you have something on that?

GRANT: Yeah, I just wanted to point out that privacy is a really broad issue or set of issues. Behavioral tracking and targeting is only one narrow subset.

And creating a do not track mechanism, while I think it would be a really great start, is not a panacea. There are lots of concerns that we still have and would continue to have that would need to be addressed. Like are there some kinds of information that just shouldn't be collected at all? Are there some uses of information that just shouldn't be allowed?

Because we lack comprehensive privacy legal framework in the United States and we just have narrow sectoral laws that give more protection to your video rental records than the records of what you do online, we really ultimately need to tackle the privacy issue holistically.

And there are some bills in Congress that are at least starting to try to look at things more broadly. And we have a lot more work to do and that will take time.

In the meantime, though, do not track is something that I think we could do in the very short term. And to the extent that it would give consumers more effective control over the collection and use of their information related to their online activities, then I think that it would at least make headway in ameliorating many of the concerns that we have.

SIMPSON: (inaudible) Ginger?

MCCALL: I wanted to echo what Chris said about not -- it not being desirable to have some sort of list here. Obviously for the privacy reasons, but because of the difference in infrastructure between the Internet and what we were dealing with with the do not call list, you would have to have some other sort of mechanism, which is why the browser plug in seems like a good idea.

But what this ultimately hinges on, though, is having some authority, some agency that actually has enforcement authority and chooses to wield that. Which is the problem that we keep coming up against with the FTC. And this is why Google and Facebook continue what we would argue are certainly nefarious deeds -- because they continue to get away with it, because there isn't any real enforcement by the FTC against them.

And so there's this culture of unaccountability, a culture of self-regulation that doesn't actually self-regulate. And so what we'd known, what this whole thing changes on, is having an enforcement agency that actually chooses to enforce.

SIMPSON: These are advertising companies but they are providing -- maybe, whether you agree or disagree -- what is more like a public utility. Right? If you get online, you pretty much need to Google. There's so many people using Facebook that -- for all sorts of different things.

Are we thinking beyond the do not track me list that there's a need for treating the Internet in much the way we've treated electricity, where we have a public utility commission to make sure it's accessible and available and that we're protected.

Or we've brought this model in insurance -- in California people have to buy auto insurance so the price has to be regulated.

Do you -- any thoughts on, you know, how we can move or whether we should move towards treating the Internet that way and privacy being a component of that?.

MCCALL: Well, certainly self-regulation in this area has failed, it's an experiment that the FTC has tried for many years, and it's an experiment that has not really succeeded here.

There has to be enforcement because of the lack of transparency online, because these companies are so often unfair and deceptive

insomuch as they're not really transparent with customers about the information that they are collecting, the way that information is used. There has to be some outside authority that steps in.

SOGHOIAN: I mean, I don't really want to speak about that thing but I do want to say that we expect a lot from the FTC, and I've work there, this is my own personal opinion, but they have actually very narrow authority.

Something has to be unfair or deceptive, and it's really, really tough to prove harm. And so we're left engaging in these mental gymnastics where we say that companies lie to consumers in these privacy policies that consumers didn't read. In fact, the Department of Justice just argued last month in Texas that consumers don't read privacy policies and -- actually that consumers do read privacy policies.

It's strange that Justice is arguing one thing while the FTC is basically acknowledging that consumers don't read privacy policies.

But if we want the FTC to be able to go out and rein in things like Street View Wi-Fi sniffing we need to give them the authority to do so.

SIMPSON: See, that's what I'm trying to get at. What is -- what is the, forget the realities we are dealing with in Washington right now. I mean, I think there's the reality that both parties would like something that's supported by 90 percent of the public -- but what is the ideal for privacy protection? Does it exist in Europe, does it exist anywhere online that treats the Internet in a different way than we do in America. more than just the cops and robbers very narrow, "Hey, the code says this"?

SOGHOIAN: Well, as a start, how about staffing the Privacy and Civil Liberties Oversight Board that has been empty for the last few years. Right? What about staffing that up, giving them subpoena power, and then sending them out to do work?
I mean, you know, I was the first technologist ever at the FTC's Division of Privacy and Identity Protection. Give them a bunch of money, give them some resources and broaden their power and send them out to...

SIMPSON: What would the broadened power be? I mean, that's what I'm trying to get at, you know, is what is the -- what is -- what is the definition of how privacy should be defined online for the consumer. I mean, we probably agree on this panel that information --

our information should be within our control. But what are the laws that are needed to actually accomplish that beyond this mechanism?

SOGHOIAN: So had Google told its customers, "We are sniffing your network," there would be no deception hook. Right? And then to get the unfairness hook you'd have to show that Google was basically not only sniffing the passwords, but then using them to log into your bank account and steal your money.

That doesn't seem like an ideal scenario. We shouldn't have to rely on companies lying. I think there are some things that we can agree that companies shouldn't be doing and I think the FTC should be empowered through rule making establish what those things are and are not.

SIMPSON: Susan, do you have something? Should we go to the audience with questions...

GRANT: Sure. Well, there was an effort recently to add to legislation expedited rulemaking authority for the FTC. The FTC is one of the few federal agencies that can't just decide that there's a problem and do rulemaking, but either has to go through a long, torturous process that can take so many years that -- to go through that the issue's moot at the end or needs congressional authority.

As you pointed out, the authority that the FTC had to act in telemarketing from Congress was obviously very helpful in creating the Do Not Call registry. There's some question about whether the FTC would have been able to do that absent that legislation.

And so I think it's clear that the FTC needs stronger authority. It's also clear that this will be strongly resisted by business. It was the Chamber of Commerce and others who successfully fought against expedited rulemaking for the FTC in the last go around and declared that a major victory.

Not a victory for consumers, and I would argue not a victory for businesses either since it prevents the FTC from adequately setting rules for the road that help guide businesses as to what they ought to be doing. And there are businesses out there that sincerely want to do right and that want to know how to do it, and I think that the FTC could be more helpful if it had more authority.

SIMPSON: Any questions?

QUESTION: Charlie Leocha, Consumer Travel Alliance.

I just want to echo Susan's comment, and this is -- I've been working from the other side trying to look at trying to bring travel under the FTC's control. And as I learned, the FTC has no regulative authority. The FTC has no -- you know, has enforcement authority based upon what -- this unfair and deceptive practices, but that's it.

And it's kind of similar to what the DOT is faced with, but I think DOT actually has more teeth to deal -- you know, more force of law to actually -- they've got regulation authority in some areas, but they're not interested in privacy.

So I'm sort of -- we're in a chicken and dog -- chicken and egg routine. And I think that somewhere finding a way to -- and a path toward some sort of regulatory authority for the FTC is a direction we have to move in. Otherwise, we're just going to be in this same kind of opt-in, voluntary privacy system which we're already in and we'll be having lots of roundtables and we'll have lots of discussions.

But I don't think any real changes are going to come until someone is empowered to do the rulemaking in this field. And that's where, if we have to put together a brain trust to figure out the best place to aim, that's what we have to aim at before we can -- otherwise we're just exercising our free speech here. You know, to change we need to really look at where we can point our collected efforts.

SIMPSON: While he's passing the mike, any models anywhere in the world that America should have? Is there a model online privacy (inaudible) anywhere in the world that we could say we want to aspire to?

SOGHOIAN: I mean, the Europeans have power and don't use it. The Canadians talk a lot about good stuff but I haven't really seen them fining companies. Given the limited...

(AUDIO GAP)

SOGHOIAN: ... power the FCT has, I actually think...

(AUDIO GAP)

MCCALL: ... some sort of articulable or monetary harm from a privacy violation. So if you look at things like the Video Privacy Protection Act, you have statutory damages built in there that allow consumers to actually enforce their privacy rights for themselves in the courts. So perhaps we could look to something like that.

SIMPSON: You know, a private right of action may be -- is there a limited private right of action for most privacy violations...

(AUDIO GAP)

SIMPSON: ... in your view? I mean, I've seen -- we know there's...

(AUDIO GAP)
MCCALL (?): ... laws allow for statutory damages. And it seems like it's a particularly good idea in the privacy realm because like you said it's often hard to prove some sort of monetary harm.

GRANT: Consumers have long had the ability to bring private actions regarding telemarketing abuses, for instance, and they've used it. And I think it's had some impact on the -- on the marketplace. So I think that we need something analogous for online privacy.

SIMPSON: To Bob Gelman (ph).

QUESTION: Yeah, I'm Bob Gelman (ph), I'm a privacy consultant in Washington. I don't want to speak ill of the do not track idea because I support it. At the same time there's this little voice in my head that says, I'm not sure it's a great idea for the government, either directly or indirectly, by hook or by crook, to start having mandates about what has to be in a browser.

And I wonder if people could talk about that and whether that's a concern that they share.

SOGHOIAN: I mean with the noise we're hearing about Kalia 2 (ph) and about the government trying to force backdoors in encryption programs there's certainly a good reason to be suspect of such mandates.

You know, I think with regard to Kalia (ph) most of those conversations are happening in back rooms and the discussion isn't can you get a back door in there it's how much are you going to get paid for putting it in there. I mean the telcos took $500 million during Kalia 1 (ph) for upgrading the Kalia (ph) compliant switches.

So, you know, I think this is something that can be a transparent process. I think the idea of the opt-out header is so simple -- I mean, I helped to write a prototype and it's like 20 lines of code. It's pretty difficult to sneak a back door in a 20-line -- 20 lines of

code.

I do think we should, you know, require that such mandates pass a very, very, very high bar. But given the opt-out mechanisms we have today are so hopelessly broken I don't really see anything better on the table.

If the industry groups have something better that they want to put forth I'm all ears, but the opt-out header seems to be the best thing that people have come up with so far.

GRANT: Can I address that as well?

We're not suggesting that the government would actually set the specifications, but that it would set the overall goal that browsers would have to provide a mechanism that would accomplish what we want this to accomplish.

Government plays a very important role in protecting consumers, for instance, in the area of public safety. There are requirements for things like cribs, for instance, to...

(AUDIO GAP)

GRANT: ... protect kids from their heads...

(AUDIO GAP)

GRANT: I think it would not be overstepping for the government to do this.

SOGHOIAN: Yeah. Let me just add that I don't think anyone is talking about the FTC actually designing the header. After spending a year using a government computer system I would never want them to design any feature in the browser. But I do think they can play a role in making sure that the browser vendors do put something in there, even if it's up to the vendors to figure out how the header works and what bytes are actually sent over the wire.

SIMPSON: So it's about 40 minutes and counting until we know what's in the report, but what do you envision the process for creating the browser might be?

SOGHOIAN: I'm not going to speak about the report, sorry.

SIMPSON: OK. Any other questions?

QUESTION: Jules Polonetsky.

SIMPSON: Wait for your microphone please.

QUESTION: Jules Polonetsky at the Future of Privacy Forum.

When Jeff's here I know if I don't say, "the industry funded," he'll add that qualification. So I...

(CROSSTALK)

QUESTION: ... so I say that, thank you.

So the initial report that really put do not track on the table in November '07 at the FTC event was one that a number of groups signed onto and it called for the FTC to create a list of domains and would require companies who did advertising or tracking of some sort to go and register themselves and then the browsers, the mechanisms that might be created by browsers would go there to get this comprehensive list.

Is that -- so when people talk about lists I'm sometimes confused. Clearly, I don't think anybody ever meant users should put themself on some list of unique I.P.s or entities that didn't get tracked. But is there still the thought that there needs to be a list that the FTC would create of and that companies would go to put themselves on this list of trackers and the browsers would go ahead and fetch that list?

GRANT: No, our thinking has really evolved over time. The browser-based solution that we've been describing today is just a lot easier and also has the advantages of not having to worry about security and other issues.

SOGHOIAN: In addition, the problem of that list is that it has to be updated, and a header doesn't have to be updated, it works whether there's 10 ad networks or a million ad networks, the same header keeps getting sent out. So it scales and it's more future proof I think.

SIMPSON: Any questions? There's one over right there.

QUESTION: Jeff Morley, Inside Google (inaudible).

Maybe a two-sided question for Ginger. Who would you recommend

authorizing to take such an action to make a browser-based mandate? Which agency would -- should be handling this in your view?

And the opposite side of the coin, if such a thing did happen what kind of legal challenges do you think that the advertising industry or the browser manufacturers might make to prevent it?

MCCALL: I'll actually kick the first part of that question off to Chris probably, but I think probably we'd see the same sort of legal action that we saw with the do not call list where there would be some sort of challenge based on corporate, First Amendment rights.

Yeah, I don't see the industry here going quietly. I think that probably there would be some legal challenges to it, and a legal challenge to the authority of whatever agency would be overseeing.

SOGHOIAN: So let me clarify that I'm a computer scientist not a lawyer, so...

SIMPSON: Ginger is a lawyer.

SOGHOIAN: ... but in the limited bit of the law that I do understand, I don't think that the FTC currently has the authority to create the do not track mechanism, to bless one or to pull companies and ad networks that's able to get them to adhere to it.

So I think we're going to need congressional action, however I don't think Congress is the best entity to be getting into the details. They don't have any technologists working as staffers on the Hill. They are overstretched as it is.

And so what I think would be the best thing would be for Congress to give the FTC the authority to come up with a do not track mechanism or at least to come up with the outline for one, and -- but I think Congress should sort of -- should really sort of farm it out to the FTC.

SIMPSON: Is there a cajole -- we heard cajole -- we can cajole the companies into participating? Any thoughts on what that might mean, Susan or anyone else, about what kind of inducements there could be to get companies to participate?
GRANT: It's an interesting question, and I haven't spoken to any browser vendors about this. So that might be a good thing to do in the interim.

But I think that it's likely that congressional action would be

needed to mandate this. And I'm not a lawyer, I'm a paralegal, but I think that there is growing interest in Congress, as evidenced by the fact that there'll be this hearing tomorrow and that we're hearing from more and more senators' and representatives' offices interested in this.

So I think that if we can create the legal foundation for the FTC to do it, then, as Chris said, they can describe what's desired and companies would have to fulfill that.

MCCALL: We could also perhaps look to the FCC, just because our bad experiences with the FTC actually enforcing...

(CROSSTALK)

SIMPSON: So that would be your preference in terms of a -- someone with jurisdiction over whatever, a do not track me system?

MCCALL: Not a preference necessarily but an alternative.

SOGHOIAN: Good. But if I may add one thing. I think the fact -- so I mean the list of speakers for tomorrow's hearing I think is public. I looked through it last night and I didn't see any technical experts among the speakers. And I think the lack of technical experts speaking about do not track before Congress I think is pretty damning.

I'm alarmed that Congress isn't including technologists in this discussion. I mean, I'm glad that it's putting consumer advocates, but I think that we need to see someone with a computer science degree at that table, if not tomorrow then certainly the next time around.

QUESTION: (inaudible) from Consumers Union. So as far as I understand it the do not track mechanism would be sort of be an all-encompassing, all ad networks, everything. No tracking at all.

Do you see there being any room for sort of a middle-ground mechanism to where, you know, let's say consumers aren't really that bothered about being tracked based on their preferences for clothes or shoes or whatever, but they would be worried about health information, financial services and that kind of stuff?

So do you -- do you see there being any kind of middle ground mechanism to where I could say, you know, "I don't want you to track me based on anything I do health-related or financial services but I don't mind if you serve me up ads about my alma mater," or something like that?

SOGHOIAN: So if you listen to the Network Advertising Initiative, they paint this fairy tale of consumers going to the NAI home page and looking through the privacy policies of different companies and saying, "Oh, well, you know, Yahoo, I really like their privacy policy. But Blue (inaudible), their privacy policy sucks. So I'm going to only opt out of companies with bad privacy policies."

Like, this is a fairy tale. The mechanism, whatever it is, should be easy to use and it should be on or off.

(AUDIO GAP)

SOGHOIAN: ... anything else is...

(AUDIO GAP)

SIMPSON: ... sounds like this report's going to address. But then when we get to the other side of it is, how much can government say, "Hey, turn on the off button," which...

(AUDIO GAP)

SIMPSON: ... off, and how do you modify it? Or do you -- would there ever be a reason to modify it?

(AUDIO GAP)

SIMPSON: ... you have one company have an advantage in terms of marketing.

I mean this is the argument for regulation, is that if a regulator keeps a playing field even and no one gets an upper hand because someone's undercutting the others through a more unscrupulous practice.

So I guess the question is what -- is the playing field give consumers total control to say, "Look, I never want to be tracked," or is there a middle ground. And you're saying there's no middle ground.

SOGHOIAN: I mean, I think with regard to the race to the bottom, the reason it's a race to the bottom is because we're using software provided by ad networks and consumers don't understand that relationship and they don't understand all the information that's going out the back door of their browsers.

GRANT: My answer to that is I don't know. If you think of telemarketing as an analogy, consumers who put their numbers on the do not call registry can allow individual companies to call...

SIMPSON: And companies they do business with have the right to call them back.

GRANT: That's right.

SIMPSON: So this is a little -- the analogy, breaks down.

GRANT: Yeah, we've never liked the fact that companies that they do business with can automatically call them.

SIMPSON: Because Citibank has 40,000 affiliates that can call you.

GRANT: Right, right.

So would it be practical? I mean, Chris makes a good point that it's a bit different here because you're really dealing with a third party not a company you're actually interacting with to do something and that you, you know, want to have this ongoing tracking relationship with necessarily.

So I don't know. I mean if it was -- if it was feasible and made sense to have consumers be able to adjust the settings for this, somehow to do that, you know, maybe that would make sense. I just really don't know at this point.

SIMPSON: I mean, but you're -- just to be clear, the target of this is the advertising networks. OK.

GRANT: Well...

SIMPSON: So in other words it's a little different than saying, "I don't want Citibank ever to call me and offer me, you know, the best deal on a credit card."

GRANT: Yeah, but we're also concerned about first party tracking, especially because of the ability for unfettered affiliate sharing.

SIMPSON: Maybe one more question. Anyone have a good one or one.

QUESTION: When you talked about different countries that might have good data protection plans in effect, are there any states right now that are starting to put good data protection laws into effect?

Because I've found that in speaking with national companies the one thing that they hate to face is 50 different state regulations. And we can -- I brought a number of big national organizations over to my side by saying we'll look for some sort of a federal pre -- you know, a federal rule.

But is there a state rule that we can look at?

SIMPSON: I can tell you, I don't know about existing state rules, but I can tell you after today I will guarantee you that someone is going to introduce do not track me legislation in the California legislature. I mean, there's going to probably be a rash of activity at the state level over this very issue. I'm certain that, you know, our next opportunity to go to the ballot there will be people who will be interested in doing this at the state level from what information we gleaned today.

And I thought what's really valuable to me is finally the FTC is actually weighing in and moving the ball forward. Whatever they say, sounds like they're saying it's viable to do this because to date there hasn't been really an answer to the industry's claim that it's not viable and I think that's where the ball moves toward today.

I think you're going to see in the next couple of weeks an unbelievable amount of activity at the state legislative level for people who want to -- who want to try to make a name. I don't think anything exists at the state level now that's comparable. Do you guys have any good -- there is no.

GRANT: No, I mean there are a lot of state laws related to privacy in other aspects, and California's one of the most active states in this area and it's great because -- because in fact most companies are national in their scope.

What California does in terms of security breach and other privacy issues really dictates the design of a lot of business practices.

SIMPSON: We actually had one of the first do not call lists by the attorney general Bill Lockyer, and he created it and then it was replicated. And so -- I think it was done by statute actually. I think he used his power in the state to do it without a statute.

So I think the great thing is the floodgates are open for privacy ideas today. And people will look at this report and say, "It can be done. Here's a way to do it. " The federal government or Congress isn't going to act.

I know in my state of California there will be legislation moving on this and there will be talk of a ballot measure on this if there's no other action at the federal level. So it's a great point about there being a state sticks (ph) to get the feds moving.

We should take a coffee break. Any quick questions or (inaudible)? OK, thank you all for sticking with us. We really appreciate it.

(APPLAUSE)

(RECESS)

(UNKNOWN): We're going to get started again. If everyone could take their seats.

(AUDIO GAP)

(UNKNOWN): ... in the online medical marketing era.

We thought it was really critical in this discussion of online consumer protections to include a panel on medical privacy because we're really at the confluence of some fundamental shifts in medical privacy, what people expect, what people are getting in relation to what they expect, and changes in data and technology. We've seen a $19 billion shot in the arm through the High Tech Act to spur a shift from paper to electronic medical records by health providers, and that effort is up and running. Our invited guest from...

(AUDIO GAP)

(UNKNOWN): ... inadequate privacy rules, certainly in regards to medical data. So I expect our panelists will shed some light on that wild West of medical privacy and what Congress and regulators should be doing to provide consumers the protection that I believe most of us already think we have.

So we have two excellent panelists here today. I'm going to start us off with Jeff Chester, who is the executive director for the Center for Digital Democracy. You heard him ask a question earlier

about a 144-page complaint he filed with the FTC on unfair and deceptive advertising practices by the pharmaceutical and other health companies.

And he is, I believe, one of the people -- one of the few people who really can tell us just what online marketers are doing when they collect, share and sell our private information online.

So I'm going to turn it over to Jeff.

CHESTER: Thanks very much. (inaudible) five or 10 minutes till you'll gong me, right?

(UNKNOWN): Yeah.

CHESTER: Thank you very much all of you. And I want to think particularly the Consumer Watchdog for holding this event and the work of the Consumer Watchdog generally and the staff, which have made -- who have made a very important contribution over the years and including recently working with us on online privacy.

I could sort of call the session -- and I don't want to do an injustice to the very critical issue of "don't ask/don't tell," but I could call it "don't ask/don't tell." Because with the online...

(AUDIO GAP)

CHESTER: ... which they tell their clients, their advertisers, their colleagues. They don't tell the public, you know. So they hope that we don't ask and they certainly don't want to tell us.

And that's why I could -- we could have filed, and we have filed a series of complaints, but we could have filed and we will be filing on financial marketing, on junk food marketing to kids, on the racial online profiling that's going on targeting Hispanics and African-Americans and other persons of color.

We could have filed on any of those subjects and much, much more about what the industry says, on the one hand, it's doing, We're here to create a positive, quote, "health 0.20 (ph) system" where you are empowered patients, you are empowered consumers, you can express freely your concerns on social networks, and you can join helping communities.

While at the same time they have created a vast, sophisticated infrastructure based on what they've already created online in terms

of online advertising and marketing to track, target and sell our medical conditions and behaviors to the highest bidder wherever we are.
And of course this is a global system. The U.S. companies have created a global data collection nightmare. And if you look at what Google and Microsoft and Yahoo are doing in the Asia-Pacific market, for example, or what they're even doing under the guise of the E.U. in the European market, as well as what they're doing here you will see that the applications, the techniques, the services that we see here are employed elsewhere and in many cases they're deployed elsewhere and originate there.

And all the talk -- now, I do believe that we can have a win-win here. I want to go through what I did. I do believe we can protect privacy, protect consumers and have a robust online marketplace. We need to do that, otherwise there's going to be a constant struggle and people, troublemakers, like many of us here, are going to cause all kinds of problems.

But the industry has to record (ph) up, and that's why there's a role for the FTC. And I do think it's extremely important to reflect that until last year when for the first time since 2000 three -- and it's not a partisan issue -- but since a year ago when the FTC had three Democratic commissioners for the first time under the Obama FTC -- the staff at the FTC were told -- it's the (inaudible) doctrine -- never go beyond the bounds of self-regulation when it comes to online privacy and marketing.

So today and actually in seven minutes,we should actually have a kind of download stretch break at 11 o'clock for those of you who are not in the press who want to see the report, which is about to be released at 11 o'clock. Today we're going to see what will be the first reflection, perhaps, in terms of a policy statement about what a new regime, hopefully a new regime might be.

So I -- I -- so if you -- and while do not track will not ultimately protect consumers is this, and this is really the work we do at the Center for Digital Democracy. You may know we've been around working on this issue for more than a decade. We got the Children's Online Privacy Protection Act passed by Congress in 1998 and have been troublemaking in this sector for a good number of years.

Take a look at Google, DoubleClick, Rich Media web page. Take a look at Microsoft Rich Media advertising's page. Look at what they say about how they collect data through these very beguiling interactive applications and services that are pervasive.

The default for the online environment is collect. And they are using all the techniques possible, tremendous torrent of creativity, to make sure that they can collect -- even designing the applications to directly be targeted to our subconscious mind. Google, Microsoft, Yahoo -- all of them are working on the latest advances with neuroscience, neuromarketing to make sure that those digital ads in the data collection even resonate within our non-rational brains.

So quickly I said I could have looked at other.

Do I hit the black one?

(CROSSTALK)

CHESTER: And I...

(CROSSTALK)

CHESTER: What happened? Did I just shut it off? Oh, I did shut it off.

And if you go to -- if you go to -- if you go to democraticmedia.org or any of the colleagues you'll see a better copy of this. You know, I just -- I did a quick thing.

But look. And this is so consistent. I want you to think about how...

(AUDIO GAP)

CHESTER: ... Google and the others have articulated, we can follow the, quote, "online patient journey." And we can convert those consumers into customers to go to a doctor's office and ask for your brand of pharmaceutical -- frankly, whether they need that branded pharmaceutical or not. We already know that television consumer -- television advertising has generated tremendous requests on the part of consumers for branded medication.

This is television on digital steroids. So this just one of the (inaudible) they say to consumers, "We're a health site. Learn about all your -- learn about all your health conditions," but here's what they tell the advertisers: "We can profile them," you know...

(AUDIO GAP)

CHESTER: I'm sorry. We can give you access. We can (inaudible) all good for you.

What they don't tell you, what Google doesn't tell you is that in fact they have a very sophisticated online advertising business promoting their ability to track and target and convert consumers for the pharmaceutical and health industry. It's called Healthvertical (ph). And they're hiring -- you want to get a job selling Google advertising to the health industry there's a job opening in New York, there's a job opening in L.A., there's a job opening all across the world.

Same with Microsoft. They don't tell you. And Microsoft -- you can change all the browsers you want, but if you go on the Microsoft advertising site and look at their demo for Connect (ph), their new -- I hope I'm pronouncing that right, I know my kid probably wants one -- their new version of the game, you will see how they've integrated the advertising and the data collection deeply into what they call immersive experiences to get you to engage.

So on the one hand they say we care about privacy, on the other hand these companies are doing whatever they can to undermine our privacy here.
Now, online ad exchanges. See, it goes far beyond do not track. Today each of -- this is an industry that needs to be -- needs some constraints, that needs the FTC and the Congress to help it -- how long do I have -- to help it develop practices that are reasonable and consumer friendly. And the last several years we've seen the rise of online ad exchanges.

Ads now are not sold based on the content that you go to -- they don't really care about the content that you go to -- they're sold based on you. What you are, what your value is to them. And if that -- you know, content is now increasingly being created by the advertisers to serve the needs of advertisers and that raises other questions about the future of the Internet.

But these are all the health conditions that you can target vis-a-vis Google DoubleClick ad exchange. So you can get an individual person who is concerned about heart and hypertension, for example.

Here's another company -- another online ad exchange -- I hope you can -- hope you can...

(AUDIO GAP)

CHESTER: ... that is also targeting (inaudible) is another good example here.

Now, we also address the other side of the coin. Because the online advertising to consumers, a highly powerful and pervasive and sophisticated and pervasive system known as, quote/unquote, "e-date" (ph), "e-detailing" has developed.

As David Vladeck said earlier, there are thousands of sales people that used to go -- go into sales offices and sell doctors prescription drugs. Now they're able to use online, very sophisticated online , techniques. Here with this cancer track they can identify these are the key influential cancer doctors who will recommend your specific brand.

Online advertising is different than traditional advertising. Online advertising is able to take a lot of information about you to serve you very powerful multi-media applications, in their own words, to immerse you in it, and to encourage you (inaudible) all advertising does, but we think, and the industry says, based on very profound and deep ways to get you to act.

And I really believe that when we're trying to get people to act about drugs, about health concerns, about subprime loans, about mortgages and credit cards -- because the online ad industry plaid a big role in the sub-prime crisis which they think they're off the hook but hopefully when the Consumer Financial Protection Board takes office next July we'll have them address that. We have to be very careful about how these techniques are used to promote specific products that have a huge impact on someone's life.

E-detailing. So they come in and they give the doctor the flash drive, the PDR. It's live. Does the doctor know that everything they do on that PDR is being tracked so the drug company knows exactly what drugs are being ordered and requested so that the drug company then can do all kinds of targeting.

So -- and there's even a big business now in so-called electronic patient medical records...

(AUDIO GAP)

CHESTER: ... that's advertising supported that also...

(AUDIO GAP)

CHESTER: ... and we think that raises new questions of unfairness and deception, because once you try to deliberately bypass the rational decision making than advertising should not have the kind of First Amendment protections it currently does.

And I thank you.

(APPLAUSE)

(AUDIO GAP)

PEEL: ... we want to, you know, we want to work together and see what we can do about privacy. Next year is going to be really important.

And thanks to everyone that worked so hard together on the letter to the Congress about High Tech. Of course you know that we haven't seen the results that we would've liked from all the great protections that we got into the bill, but that's where we need to get together and plot for next year.

So I just thought I'd say a few brief things about the environment and then we could talk about really whatever you like.

So here we are -- I don't know, is Bob Gelman still here, he can probably tell us -- how long has it been that we've been waiting and waiting to get a definition of consent, a definition privacy.

What happened there -- OK. We've been waiting a long time, we don't have it.

This slide I still show every time I speak because so many people still don't understand that the HIPAA privacy rule was gutted in 2002 and the right of consent is no longer in it. And so the top box is some language from the actual statute, the HIPAA statute. The middle box, box inside box number two, is the policy that W. put in place when he took office and announced that he was the privacy president.

And so you can see very clearly it says that before any information moves you have to have consent for routine uses: for treatment, for payment and for health care operations.

And then if you look closely at box number three that's what happened to us in 2002. It was never ever reported and it's actually a little bit tricky language. It says consent provisions are replaced with regulatory permission for covered entities to use and disclose

your PHI for TPO.

And a lot of people missed that, and, very frankly, HHS wanted everyone to miss that. And so think about the language we hear from HHS, it goes something like this, "Only authorized users can see your information." I'm like, "Oh, thank God. Only authorized users."

But of course that's really -- that's really, you know, thousands of people because everyone's authorized. All the covered entities are authorized and you're not.

So that's -- you know, use this slide, take it. It's really important for people to understand that they don't have a federal privacy rule.

And then this other slide is the kind of the scare slide. It's supposed to give you a sense of how many different entities can see your information. In the middle, of course, is the doctor and the patient.

Then the next zone is covered entities. And we think there's about 4 million of those. Everything from a solo doctor like me to Hospital Corporation of America and self-insured employers. And then the data's shared in the zone around that which are business associates -- God knows how many of them there are -- lawyers, accountants, transcriptionists and so on.

And even beyond that is the Gramm-Leach-Bliley Financial Services Act which allows banks and financial institutions to see and use your medical records.

Now, there is an FDIC notice that says they cannot look at that information to make credit decisions. That's very comforting. But they can share it in the same way that they can share credit reports. So now you can feel really secure about that.

And we need this, I think, because it's really important to understand that the threats are certainly there from hackers and poor security, but what we really have to worry about is all the insiders that have information about us that shouldn't.

So after the Consumer Choices Technology hearing last June -- about a week after, really -- we got a pretty big announcement from Secretary Sebelius, seconded by Dr. Blumenthal, that there was going to be a new administration-wide commitment -- now, they didn't use the word privacy, but they used control, Blumenthal used control, and she

used other words, you know, that imply control.

So those are steps up, and I don't know, I take comfort from they're being said at the beginning of these people's work and reign in HHS and federal agencies instead of on the way out the door, like Secretary Leavitt. And so remind them of these promises.

And actually I've been hearing a lot about Blumenthal speaking around the country lately and he's getting much stronger. I don't know if many of you have seen, he's got a slide with a really blue ocean and a really big iceberg. Have you all seen that?

OK, so there's a big iceberg, and up at the top there's I think it may be quality or meaningful use or one of those other useless things that they're doing with our information. And the bottom of the iceberg is labeled privacy and security.

I think that's pretty stunning, I'm going to start using that slide too. But it's -- they're getting the idea that it's a real problem. And I just wanted to show you -- I'm sure you're following the Wall Street Journal series, it's just amazing. And this particular one is all about the latest type of actuarial research, which they think they can do without getting your medical records.

So that's very, very interesting. And it's back to why we've got to get meaningful online privacy because there isn't a separate environment for health data. Health data is everywhere.

And as a physician, a practicing physician, I am especially offended by what you were saying, Jeff, about health websites because I really think people have -- and I'll get a little analytic again -- a kind of a transference to anything that has health in it. Must be a doctor, must be somebody that's trying to help me. But it's not.

And so they really take advantage -- I think it's really evil to take advantage of sick people when they're scared and looking for help.

And so this is the -- this is a slide, this is Deloite Touche's slide about how to sell the system. And if you -- if you -- you know, if you look at it, you know, you kind of begin to see the behavioral characteristics of somebody that's, you know, kind of a slug and likely to get sick and somebody who's really active.

So I just thought that was pretty interesting that we're getting such great investigative work from the Wall Street Journal. And what

can we do together to get the agencies and the watchdogs that are supposed to be in the agencies to be doing some of this digging in.

And we did a poll ourselves recently, just want to tell you about it...

(AUDIO GAP)

PEEL: ... access electronic health records. Duh, no. But the public doesn't know that they're all set to be data-mined for an entire series of research premises that the public hasn't even heard about.

Well, there's of course quality improvement, there's pay for performance, there's comparative effectiveness, there's population-based health, there's personalized medicine, there's, well, fraud and abuse. Anyway, on and on.

And, you know, I don't know what you think, but that may be something that we might want to work together on this next year because what's research and what isn't is really -- many in industry and the government are making fine distinctions, that, you know, quality -- quality improvement inside the hospital, we shouldn't have to get consent for that because you want quality don't you? And you owe it to yourself and everyone else to be part of it.

But all of these things are research and that's I think how most people see them, as research, and they want to be asked to participate. And they will.

So what else do we have?

Who do you want to decide? You know, another obvious question. But we couldn't find any polls that really asked this.

So this is very useful, particularly if you're -- how many are working with state affiliates or state chapters? This is really going to be huge. If you think we're outnumbered here in Washington...

(AUDIO GAP)

PEEL: ... you can't imagine how bad it is for...

(AUDIO GAP)

PEEL: ... there was a website that didn't do anything with your

information unless they told you, would you be interested? I think everybody got confused. It's a little bit tricky, it's a kind of an unfamiliar question.

But there's still a lot of people that said "yeah," still said "yes."

And then we have this one: Who should decide about corporations and researchers seeing your information without your permission? And nobody -- you know, nobody trusts anybody but themselves really. Doctors -- 5 percent. Government through laws and regulations -- not much trust there either.

And so this is really, really important. The only other thing that I'd like to talk to you about briefly that I think is an issue coming up for us to think about is the research loophole in HIPAA, which allows hospitals, EHRs, PHRs, IBM -- anybody and their dog -- to claim that they're a researcher and sell health data.

And, Jeff, I'm glad you're a lawyer here. So I've been spinning this little theory in my mind -- and some of the rest of you are lawyers too -- OK, Goldman Sachs, right, they got in trouble with the SEC -- this new group in the SEC -- for misleading shareholders, right...

(AUDIO GAP)

PEEL: ... and the public about their real business model (inaudible). So that's not what Congress had in mind. They thought they were going to, unleash all this data for cures. But, as usual, you know, the patients and the doctors are the last ones to get any meaningful use out of this great expenditure. So...
(AUDIO GAP)

PEEL(?): ... to actually act on the wonderful historic protections we got into High Tech.

So thank you very much.

(APPLAUSE)

(UNKNOWN): Great. Well, thank you very much.

Well, I was just going to spin it right into questions now, and I'll pose a question which I'm sure you have answer to and you can respond to Deborah as well. And we if can grab the mike for questions

in the audience in a second.

I would just love to know -- we've seen a lot about what the harms are and what the practices are out there, which I believe you're absolutely right, most patients believe that if they tell it to their doctor, if they're searching to find out information about their rheumatoid arthritis online, nobody's going to know that.

So I'd like your top one -- and I'll say one because I know I'll get more -- regulatory and legislative solution -- you're top this is one big important fix. Obviously nothing will fix everything.

PEEL: For me, I still think that we need -- we need -- I think we need a law that protects health information wherever it is. So I think that the protections have to flow with the data.

If you happen to be on Facebook your data should be safe there. If you happen to be in a hospital it should be safe there.

So I would say that my top regulatory wish, and it's clearly a wish, would be that we could restore the right of consent or get a definition of privacy which we've been working on at the federal level for a long time.

CHESTER: I concur about that, and I'll just add two things.

One, I haven't been able to download the report yet so I don't know if it's out. But one of the things that many of us have said the FTC should do -- and it'll be a litmus test today -- is whether or not they identify online health and medical-related information as a sensitive area that requires greater safeguards, such as an opt-in many of us are calling for.

And two, as you, many of you know, the White House recently announced a new interagency working group with almost all of the agencies of government to develop new privacy and e-commerce policy. And I think we need to make this issue at the top of their agenda: What exactly is the Obama administration's position to protect health and medical privacy online? And confront them with that as soon as possible, which we intend to do.

PEEL: Yeah, I had the opportunity to be on an FTC panel about health information and I said essentially the same thing. We're not going to have privacy if the protections don't follow the information -- at least for health.

(UNKNOWN): Brief update. The FTC has not put their report online because they're having technical difficulties.

(AUDIO GAP)

QUESTION: ... teens and their privacy. This is a reality.

One of the things that teens want privacy from is their own parents and health information is a big part of that. And I'll go ahead and call the elephant in the room the elephant in the room: information about abortion services, for example though not the only one.

Is that really a problem here? I mean I know you've talked about advertising this information and I agree that that could easily -- that's not a conflict, but there are people from the industry side who will say if you put more protections on teens -- demanding their parental opt in for example -- you run into a real problem there.

And so teens as a special group, do they -- how do we protect their information and still give them access to all the information that they want to be able to get online?

PEEL: Oh, that's really tricky. Jeff may know more about it than I do.

You know, I think it's really important of course that teens have privacy, and we kind of crashed on the shoals of that with the conservatives that were with our coalition in 2007. They were very much in favor of control of information, and then the, you know, the anti-abortion wing of the party...

(AUDIO GAP)

PEEL: ... was the eleventh hour and we couldn't say, "Well, OK, guys, couldn't we like carve that out, maybe, and leave it where it is at the state level for now so that all of the rest of us could have the (inaudible)."

Anyway, so that's kind of what happened.

But the problem with teen privacy is a big conundrum for electronic records. In fact a lot of them -- you know, it's a giant hole. They won't even collect teen records. And so -- because they're struggling --struggling with that.

But, you know, we need to find ways for them to get the information, get it privately. It's ironic, you know, maybe online they can keep their parents from knowing, but the rest of the world knows. You know so -- where have you gotten.

CHESTER: Well, Alan (ph) knows a number of leading groups, including Consumer Federation of America and Consumers Union and World Privacy Forum and many others have asked the FTC to develop special rules for teens, and I think -- what I hope we will see in the report today is recognition that teen are indeed a sensitive category.

The coalition of groups, many of which lobbied through the Children's Online Privacy Protection Act, are not calling for the same parental control if the child is under 13. But we're calling for a kind of opt in transparency for specifically designed teen sites that would give the young person much more -- basically the same kind of protections we'd like to see for adults where they'd really be told going on, et cetera.

So we're going to continue to push that.

Clearly, in terms of medical information, that does raise critical questions. But to me one of the most disturbing aspects of doing the research -- and I've looked at online pharmaceutical marketing for two years -- took me a long time to get this out -- one of the most disturbing aspects was how they -- how some of the drug companies were using online to target parents to get the parent to ask the doctor for a specific anti-schizophrenic medication for their child or teen. A deliberate strategy to push the parent over the edge to get...

(AUDIO GAP)

CHESTER: ... kid medicated, whether the kid may ...

(AUDIO GAP)

QUESTION: ... to the extent that somebody Googles breast cancer, is that not something that a do not track mechanism would capture and is that sensitive health care information?

CHESTER: Look, I think that clearly the action of the search on its own raises the question about whether or not it is sensitive information. It may depend on the condition being searched.

But given the fact that the online marketers have created what

they call the tracking of the, quote/unquote, "online patient journey" -- and it's a whole -- when I raise these questions about do not track -- the industry has created and continues to create a very holistic system to get people to opt in. If you're going to want to get the content, if you want to get the discount, you want to hear that pleasing video, you know, blah, you're playing with that game -- the industry has got it worked out so you'll opt in.

But I think we need to get -- in terms of developing and thinking about the sensitive safeguards -- we need to think about the actual business practices, because now it's the capture of the first search. It's then targeting you with advertising to get you to look for a specific condition. It's all in the report. And then it's targeting you to go to the doctor and ask for treatment.

Why? It's a holistic system. And we need to address how to protect the consumers' rights around that system.
PEEL: Yeah, I would just say, I think, too, a new -- I'm sure you covered this -- but, you know, everything is being combined with everything -- so what you do online they're going to combine with credit card stuff and what stores you go to. If your car GPS could tell them which doctor's office you went to or whatever.

So it's -- I think most of the public doesn't really understand how easy it is for very sensitive and very highly predictive profiles to be built.

I mean, I'll never forget when the Republican chairman said -- I think it was when Bush was in he said something like, "And we know who our voters are and they are not the latte drinking, Volvo driving, yoga practicing, sushi eating..." -- oh, my God.

And so it's amazing the kinds of things that they're targeting. And I'd like to see us put an end to behavioral targeting in politics so that people would have to talk to each other.

(UNKNOWN): I think we have time for one more question, if we've got another one out there. I of course have one, but if anyone else has a question.

(UNKNOWN): Well, I would just like to add to I think what Aaron (ph) said which is that personal health records...

(AUDIO GAP)

(UNKNOWN): ... the stuff that your physician writes...

(AUDIO GAP)

PEEL: ... like psychotherapy records -- you can't return it to privacy again.

And so they're pushing these systems at the state level that I believe really do -- really do violate existing rights and state laws and constitutional law and the rest.

I'm not a lawyer, but -- oh, this reminds me of one other thing.

OK, all you lawyers, OK, many years ago before I started Patient Privacy Rights, when Bush eliminated consent, a group of us really active Freudian analysts -- it's a joke -- anyway, we got together and we decided we had to do something because we couldn't -- you know, nobody knew what happened.

So we filed a federal lawsuit and we accused HHS of eliminating our fundamental right of consent. OK. Well, it went up and up and we didn't -- we didn't win...

(AUDIO GAP)

... they didn't take it at the Supreme Court. But the reason (inaudible) and so essentially our case was, "Look, if we have a right to consent, a right to privacy, how come we have to beg somebody and they can say no? "

That's what we thought the case was about. But the Court said there was not state action, OK? We have state action now. And this is what I want to bring up with you. Now every physician, right, in every hospital, and all of us were supposed to have electronic health records by 2014.

All of the systems, all of these electronic systems deprive us of the right of consent. You can't give meaningful consent in these systems. And so we now have, I think, state action because, as a physician, if I don't adopt this and get my incentive money, then in a few years, then they penalize me.

So we have -- we have state action now, and all of the arguments, right, or the things that you do in court, filings and whatever, all of those would still apply. Only now we really do have state action.

Essentially, they told us, well, you should -- you should go file

your suit against the pharmacy; that's who took your rights away. And, you know, we were broke and all that, and we couldn't do it, so -- but we do have state action now, if anyone is interested. And the same 750,000 patients from all 50 states would very likely want to participate -- so just another possible strategy.

CHESTER: Just quickly, two things. Once is, once again, companies like Google and Microsoft that are offering electronic patient health services, that have built a very sophisticated business selling pharmaceutical and health advertising and targeting consumers of Google and Microsoft and the others need to know, at the very least -- I frankly think there's a conflict of interest -- but all the ways they're selling, targeting these -- the health conditions, too.

As we say, in the complaint we have companies like Practice Fusion that are going around and offering physicians and advertisers supported-based electronic patient record. All kinds of data is collected. They're even telling the doctors they can go and apply the stimulus funds and make money in the advertising. So clearly we have to see a crackdown on the whole electronic patient medical record industry.

(UNKNOWN): Well, I wish we had more time, but we have to go download a report. So I appreciate very much both of you coming. We'll take just a short break to switch out panels, and we've got John Simpson coming up.

(CROSSTALK)

SIMPSON: The short break is going to be just as we all come up. We are in fact, as you know, webcasting this, and we've got the schedule out there. And quite literally we think people around the world are going to be expecting to tune in at 11:30 and -- and hear this panel. So we will try to go right on the schedule.

I'm John Simpson. I'm director of Consumer Watchdog's Inside Google project. And we have been critical of Google in a number of areas. Part of the thought, of course, was, but by focusing on a specific company, it helps educate consumers in general about some of the online issues, privacy issues and that sort of thing. Also, because Google is such a dominant player in the Internet world, we felt that by cajoling and persuading and other sorts of things, we might actually get them to adopt some appropriate practices in the area of privacy protection and that kind of thing, and that could then potentially set a gold standard for the rest of the industry.

As we got involved in some of these issues, we got intrigued by Google's size, power and dominance -- I would say monopolistic power -- which we think they exercise a lot.

And we've had some reports out on this. I was here in April. At that time Gary Reback joined me, when we were calling for the Justice Department to open an investigation. Justice still has not done that. They did oppose the open book settlement case, which we had encouraged Justice to do. We filed an amicus on that as well. And as you all probably know, the European (inaudible).

(Inaudible) is a well known antitrust lawyer. I guess you could say, at one time or another, he's probably represented most of the prominent Silicon Valley I.T. companies in one way or another. Last year he founded the Open Book Alliance, which is opposing the Google Books settlement. He's of counsel to the litigation practice group of Carr & Ferrell and specializes in intellectual property law. He's probably best known for authoring a widely read white paper successfully opposing Microsoft acquisition of Intuit. And he was a counsel for the so-called anonymous amici opposing the Justice Department's first consent decree with Microsoft.

I guess you could say he is generally credited with spearheading the efforts that lead to the antitrust action against Microsoft. Now it's a decade later. Some of us would say we have a new Microsoft, and he is very interested in what Google is doing. And I think we'll let him speak for what he thinks should happen.

We're really pleased that Melanie Sabo finally finished jury duty. Some of you in this area may have in fact seen her in that regard. She has joined the Federal Trade Commission Bureau of Competition as assistant director of the Anti-Competitive Practice Division. She previously was a partner in the antitrust law and trade regulation practice group at K&L Gates. She's been in the antitrust division of the United States Department of Justice, served as Counsel of the Antitrust Subcommittee of the Senate Judiciary Committee and clerked for the Honorable William J. Castagna.

I probably should say this. I suspect you will say it. She is in fact from the FTC, but she's not speaking for the FTC today. She will be offering some of her own personal opinions about the sort of legal challenges and antitrust issues around the Internet. And I think it's important that we say that because some of us are trying to get Justice and FTC as organizations to act officially. So she's here in an unofficial capacity with her own opinions.

So I guess, Scott, you're going to start us off.

CLELAND: Thank you, John, for hosting this and your organization hosting this.

I have testified on Google antitrust both before the House and the Senate. I also work, as he mentioned in the intro, for companies. And some of those are for competitors, so you should know exactly where I'm coming from.

I also wanted to refer you to my presentation that is in the document. It's the only one -- it's colored and it has numbers, and I'm just going to point out a few slides to you. And I wanted it in the deck so you could take them in the future. But I'm going to make a couple of points briefly and then point them out and you can go look at them more in detail later.

But the main point is Google is a monopolist. We know that from DOJ, when Google tried to do the -- the Google-Yahoo ad agreement. Then antitrust chief Barnett, who was not considered a strict trust-buster, threatened section -- Sherman section one and two, anti-monopolization case, against Google. And they felt they had a case and would win, according to Sandy Litvak, the prosecutor -- that would have been the prosecutor on that.

So the DOJ does believe that Google is acting as a monopoly. We learned yesterday that the -- that the E.U. is investigating Google.

Now, we know implicitly; it's obvious that they believe that Google is a monopoly. What they're -- because all of the things they're investigating wouldn't be a problem if a competitor did them. We wouldn't even have the investigation. So what they have to do is find out can they prove those items and are those anti-competitive?

But both the DOJ and the E.U. understand Google is a monopoly.

Now if I could ask one question of the audience, just who in the room uses Google?

I think most everybody in the room is -- is raising their hand, and that's, you know, more affirmation that, you know, Google is very widely used. I wouldn't call them big; I would call them pervasive and omnipresent.

Now, what I want to do here is do a very quick overview, kind of, a big picture, helping people understand what's going on. What I

wanted to do was point out a few slides. And that was -- because the problem is not that Google is -- is big. And I like to say big isn't bad. It's -- you know, but you have to understand Google is the most powerful company in the world and -- and in history. And they are increasingly becoming the Internet.

So I have a slide in here that would be on page 18. And there's a lot of small print. I don't expect you to look at it right now. But I, in my latest presentation, Googleopoly VI -- and I've been writing about this for three and a half years. I've written more about Google antitrust than anybody in the world. You can find over 200 pages of antitrust research on Google at Googleopoly.net.

But what I've done here -- and I did this this summer, and obviously, this was presented to all of the relevant antitrust authorities -- was to give them an understanding of how pervasive and omnipresent Google was at every single conceivable layer or element or facet of the Internet.

The next thing I want to point out to you is the slide on page 20. You may have heard about the issue of total information awareness that was banned by Congress when the DOD decided they wanted to try and track everything that happened. And the Congress said, oh, that's not a good idea.

Well, this slide here shows that Google has already achieved it. And when I did this exercise last spring I was personally stunned when I compiled and catalogued all of the things they do to collect in all of the different directions. They are omnipresent. They are pervasive. And they are omnitrackers of a mind-boggling amount of action on the Internet, most everything that -- you know, over 1 trillion web pages, over 1 billion people, on and on and on. So to study that one -- and it will -- it will, I think, trouble most people.

The next thing I wanted to do is to go to 24. This is the only slide I'm going to actually go through. But this is basically to try and help you understand. You know, people say, well, what is Google doing wrong? You know, they're just big and they're -- they're (inaudible) say, what's wrong with what Google does?

Well, first of all, as I show on page 24, Google self-deals itself aces that are hidden in its sleeve. They manually rank Google-owned content first, maps, YouTubes, mobile, despite representations that Google never manipulates search rankings to put partners higher in their search results. I think themselves -- you know, they would

consider themselves partners.

Google deals its competitors bad cards, opaquely, from the bottom of the deck. Now, Google has human raters that opaquely and mysteriously assign quality scores so that certain competitors rank lower and they -- or they have to pay more to get traffic. And you've heard Foundem, myTriggers, EJustice.fr, CHOW, and others -- Navx -- that have had this problem. So it's not an isolated incident.

Google sees and counts everyone's cards, so they can't lose. Only Google tracks all the (inaudible) information, connections, interests, click paths. Only Google profiles and categorizes each user into demographic segments. Only Google can reverse-engineer publishers, audience and advertiser lists to create Google content, products, services that can front-run or skim those competitors.

It's the only -- only Google knows all the advertiser demographic information so they can front-run publisher partners with Google-owned content, products or services. They know everybody's cards.

So it's like a card game where they have a video that's looking over everybody's shoulder. They know it all. They're watching every -- you know, they're -- they're almost being able to monitor perspiration and, you know, whether someone is heating up. It's almost like a lie detector test out there. They know most everything. They -- Google alone decides who can play -- play which hand, and what the specific ante is in whatever event.

Google alone decides who can bid on which keywords and they set minimums, price minimums. They run a black box.

I actually heard NPR today say, "Oh, it's not a black box. We're actually very transparent." I don't think so. They exclude competitors from the game (inaudible) who could spot Google's double (inaudible).

All these things that go wrong -- well, wait a minute. That happened. I guess that would be considered a problem that, if you have somebody who runs a market and controls a market and sees everything and no one is watching and no one is policing, I think we could say that that could go off the rails and there could be some problems.

And also think of, you know, derivatives as algorithms. And all of these markets I'm talking about are algorithmic markets.

I'll just refer you to, briefly, now, page 23. That's in antitrust speak, what I just said in laymen speak. But that is -- you know, people say, "Well, what have they done wrong? You know, they haven't done anything wrong."

Well, here on one page is laying out basically their monopolization strategy.

The next thing I want to do that will help people understand the big picture -- and I want to be sure I'm not using too much time here -- is just page 27, what I've done here for you -- I have a mechanism that helps people understand Google has its monopoly platform of power.

It gets -- all sorts of constant acquisitions around it to protect itself. Then it has satellites like AOL and Ask.com, where they basically do the search for those, and they're basically satellites because they depend on Google. And then they have partners, everybody who revenue-shares with them on AdSense or AdWords. They're partners. And then you have this free zone, which I basically call this napalmed, dead, free area, where they basically want to put out free products in all these markets where everybody else offers, you know, for-pay products that no one can compete with. And then outside you have, kind of, the gray area of competition.

So this gives you a sense of the overlapping spheres of monopoly influence. And then I just, on page 28, I show how they can do that to discriminate. And then on page 34, if you want to know, I just came up with 200 companies that are in Google's monopoly path. You ought to -- if you want to look at all the industries, I came up with about 20 and about 200 companies. It affects a lot of people.

Now, briefly, I want to set the table on ITA because that's a very important pending transaction before the DOJ right now. And first what I want to tell you is -- who is ITA?

Well, you can really simply think of them -- they're the Google of travel search. They do travel search better than anyone. ITA does the underlying search engine traffic -- your know, all the search engine and algorithmic stuff, and they're the best. Google wants to buy them because Google can't do it. They're the most innovative and -- and the best.

To tell you and to prove to you that Google -- that ITA is the Google of travel search, every online site after 2001 -- every single one that wanted to use a travel search engine chose ITA -- every

single one.

All right. So they have about 65 percent of the market. They don't have all of it and whatever. But they're viewed as the best. Before Google wanted to buy them (inaudible).

And they have almost all of the advertisers in the world, over -- about 1.5 million. And they have all of -- almost all of the web publishers that matter. So they have all of the relationships that anybody would need to compete in the travel vertical.

Now, I don't like that term travel vertical. This is the travel sector that happens to be in the online space. And so when you put the company that has relationships with everybody and tracks everything and you tell them they want to buy ITA, which is the Google of Internet search, you should scratch your head and go, "Why do they want to do that?"

They want to do that to control things. Because if they didn't want to control things. Because if they didn't want to control things -- ITA said, "We'll license to you. " Or Google could innovate and get better and do it better than ITA. Or Google could compete with ITA. Now, that's -- that's an idea right there.

So that's basically telling you a little bit about ITA. But I also wanted to mention that it appears in the press that Google is about to pay $6 million for Groupon, which is a consumer, kind of, social networking coupon space for the local market.

Well, that -- that is going to be a big deal. Just think of Groupon as, like an ITA is to travel, Groupon is to the local market. And so I want to leave you -- remember, with Microsoft, what the Department of Justice did is, when they blocked into it, they realized, wait a minute; we have a horizontal monopoly here and it wanted to reach out into finance. And DOJ blocked it and basically said, "No, we don't want you to do it. "

Well, unfortunately, the FTC didn't follow that wisdom and they allowed DoubleClick to go through and AdMob to go through, and so Google is saying, "Hey, this is a stop-us-if-you-can mode. You know, DOJ and FTC and all those people haven't stopped us yet, and so we're going to take whatever we can. We're going to go into all these sectors and we're going to extend our monopoly as far as we can until somebody stops us."

And so that's where we are right now. And I'd like to pass it

over to Gary Reback.

(APPLAUSE)

REBACK: Can you bring my presentation up?

You want me to -- there you go. Thank you.

Good morning, and thanks for coming out on what is a -- a stormy day in Washington. You know, I've got a lot of information today that I'm going to have to rocket through, including some data that's brand new, off a big study that I've been doing. And so I'm not going to have time in this brief presentation to even give you all the examples I have, because I want to show you screen shots and I want to illustrate some of the points that Scott made and some other points so that you can see them, because hearing them is sometimes confusing.

You know, when I make this kind of presentation for a Silicon Valley audience, the -- particularly if they're in the companies that are affected by Google's conduct, they understand instantly in a half a sentence the point I'm trying to make. But for real people, it's a little bit different. And so I'm going to try to take it slow where I can and rocket through the rest. And if you want to know more or have some questions afterwards, by all means, please come up.

I want to say, at the end of this, if I can get that far, I'm going to have some fairly harsh words about the lack of the Department of Justice's action in this matter.

And the reason I'm raising that right now is I want to say that I'm not talking about Melanie Sabo, who doesn't work for the Department of Justice and is here presenting her own views. She works for the Federal Trade Commission. I am particularly grateful that she has agreed to participate on this panel. Earlier this year she gave a very interesting presentation in Florence, and we asked her whether she'd give something like that here. She's speaking for herself. But I just want to make that clear. I think you'll understand who I'm talking about when I get to that point in the presentation, but I'm not talking about -- I'm not talking about Melanie.

Now, I think, as all of you probably know, just yesterday the European Commission, which is the administrative branch of the European Union, said that they were launching a formal investigation because they'd received complaints that Google is abusing its dominant position in search by placing links of competing search services lower in Google search results than they otherwise should be, while at the

same time placing Google's own search results higher than they should be using a neutral algorithm.

In other words, Google, the investigation goes, penalizes competitors' competitive search results and preferences its own vertical search results. "Penalties and Preferences": that's what I'm calling this presentation.

So, as you know, taking one step at a time, when you type a query into Google.com you get a bunch of (inaudible) specialty search engines sprang up.

And Scott mentioned some of these. These are specialized in things that we call "verticals" or "sectors" that Scott said, specialized search engines to help you find the lowest airfare, for example, or the best restaurant in your area or the lowest price for a particular consumer product.

You know, a specialty search engine doesn't work on relevance because that wouldn't work. And I'll give you examples of how they do work. But the important point to understand is that they work on a different set of algorithms than Google's general search does. Now, these -- these specialty search engines really satisfied consumers who were looking for special answers to special kinds of queries.

And Google found that, when Google directed traffic to those sites because they came up high in relevance rankings, consumers went there and they were very satisfied and they didn't go back to Google for their next search; they stayed on those specialty engines for their next search. Once they found the airfare, they wanted to find a hotel. They didn't go back to Google. They stayed on the specialty sites.

Well, that was poison for Google because the specialty sites were able to sell ads, and Google wanted to sell those ads. And more than that, the specialty sites began to grow and grow -- specialty engines -- and Google became concerned that they would grow, at least collectively, so much that they would erode Google's stranglehold on general search.

So Google decided it was going to change its business plan and it was going to take out these nascent vertical sectors. And so back in approximately 2004, it decided to go into business in these specialty areas that it hadn't done before.

Now, what's wrong with that? It goes into specialty areas.

Well, probably nothing -- probably nothing. But the problem is (inaudible) did that, but that's not where it stopped. It took its own results and preferenced them in a general search, and I'll show you some examples, so that competitors were disadvantaged and it -- eventually it gave a name to this initiative. It called it Universal Search, and they gave it that name about in 2007.

Now at roughly the same time, in fact a little earlier, Google started using techniques to change its algorithms to also penalize these specialty search engines so that they appear at a lower rank off a general search than the normal relevance algorithm would place them.

Now, this created a lot of controversy, and Google wants to debate this point. Generally speaking they say, "We, Google, need the freedom to penalize spam, for example, or to put lower-quality content sites lower than, say, the New York Times."

And, of course, all that's true. But, that's not the concern. The concern is Google is hiding behind those...

(AUDIO GAP)

They developed a particular association with groups involved in specialty motorcycle accessories and parts in the U.K. And so, if you did a search for this particular kind of motorcycle helmet on Foundem, you'd get a whole lot of information, and you'd be able to compare prices and decide which merchant you want to buy this product from.

Well, Google -- Google decided out of the blue one day in 2006 it was going to penalize Foundem along the lines of that policy that Matt Kutz (ph) indicated because Foundem was, in fact, a search site.

And so, it -- instead of having Foundem very high in the results if you did a search for this motorcycle helmet, it put them down at about 1,000, meaning you're scores of pages down. No consumer would look there. Foundem raised holy hell. They went to the press, and Google raised them back to position 145, still way below any consumer -- where any consumer would look.

At the same time, they were penalized and ranked at position 145 by Google, they were ranked number one by Yahoo! and number seven by Bing. So, they went to the European Commission among other companies...

(AUDIO GAP)

... its own, not just penalizing competitors, but preferencing its own results in comparison shopping. And I want to give you two quick examples of this. I don't have a lot of time to do this justice, but I want you to see what's going on.

So a long time ago, there were sites that sprang up, I'm using Yelp here, but City Search is a good example or Trip Advisor, to help you choose the best local restaurant for you of a certain kind, or the best local attraction, or the best park or the best hotel or whatever it is.

And generally speaking, these kind of sites rank merchants, hotels, restaurants by consumer reviews, star ratings, written reviews. And, of course, if you're looking for the best restaurant, that's exactly what you want.

And so, as I say, I'm just using Yelp as an example here, back in 2004, Google decided it would go into this business. And so if you did a search off Google dot com, I've used pizza in Redmond, Washington, right at the top, ahead of everything else, you'd get...

(AUDIO GAP)

... three restaurants listed there that...

(AUDIO GAP)

They're giving you what they think is the best restaurant, not the best restaurant under the notion that you might pick a best restaurant. And I'm just going to illustrate this very quickly and move on.

If I did a search for -- I did this search last week, so it's maybe different today -- but if I did a search for Indian restaurant in San Francisco, this is what I'd get out of Yelp.
Now, just kind of observe the restaurants, because if I did the same search on Google dot com, this is what I'd get. Now, Google doesn't even have a box up there anymore, so they don't tell you they're preferencing these restaurants according to their own local search. They just start listing restaurants.

But you'll notice, these restaurants aren't the same as the last restaurants. Now, Google has started putting in customer reviews. They have some of their own, but they've also just been taking the reviews from other sites, with or without their permission. There's a lot of controversy in the industry about that.

Eventually on the second page, you get down to Yelp, down here, and you would learn if you clicked through that Yelp has a different listing. But -- so, the issue is what difference does this all make?

Now, I don't know how many of you saw this article on the front page of the business section of the New York Times on Sunday, but it points out that merchants that -- at least in this case, using this as a representative case -- merchants that abuse their customers, online merchants, get a lot of nasty reviews.

Those nasty reviews count as relevance hits, and so boost the merchants' results on Google. So this guy, this particular guy, was abusing -- according to this article, I don't know personally, according to the article was abusing customers and getting a higher rank in Google.

And of course, under the other kinds of sites, under Trip Advisor or City Grid or Yelp, would be ranked quite differently. So, that's just a quick -- that's just a quick example.

I want to now focus with the little remaining time I have on the real reason that I came here, which is to talk about the same problem in comparison-shopping engines. And, I -- this has been big news out where I am, and I'm sure it's big news here, too.

Now during the holiday season, if you have a smart phone and you're standing in the store you can aim -- you can use some of the software that will read barcodes, or you can just take pictures of a product, invoke one of these -- what's called comparison shopping engines, and it'll tell you whether there's a better price for the product you're looking at, right as you're looking at it. And so, that's kind of a big deal.

Now, who makes these comparison-shopping engines? Well, I have on -- Foundem is one such example -- but I have on the screen in front of you sort of the main players in the United States. And I want you to understand that there's a difference between these kinds of search engines, specialty search engines, and merchants.

Amazon, for example, is a merchant. Wal-Mart is a merchant. Google is forever telling people, "Hey, Amazon still outsells us on the web," which I suppose they do, but Google is not trying to get rid of merchants. It's trying to get rid of these guys.
So, here's the analogy. If I go to Safeway in search of the cheapest breakfast cereal, I could make a comparison of what's on the

shelf in Safeway and I'll get the cheapest price at that particular Safeway, but I won't get the cheapest price everywhere. And that's what these products do, these services do. They allow you to compare across the web and to get the cheapest price.

So, this is just a representative example. There are millions of examples. But if you do the search on google dot com, compare prices, and I have a camera there, you get a set of -- right under the paid ads, you get a set of results. They aren't even indicated as Google shopping results, even though they are.

You think, the consumer thinks, they're just shopping results. Well, in fact, they're Google shopping results. They come there first with three examples, and then everybody else is relegated to a lower position.

And if you're familiar with positioning, you understand that the first slot is worth twice as much traffic as the second slot, and the second slot is worth twice as much traffic on the third slot. By the time you get down to slot eight, nobody's going to look at you. OK. So, this is an example of what this problem of preferencing means.

Now, when people make a search, trying to do a comparison-shopping analysis, sometimes they do it the right way, as I indicated back here. They do compare prices, blah, blah, blah. But, for the most part, people just type in a product, something they're looking for, and hope Google dot com will get them the right -- the best comparison-shopping results.

Well, companies like these comparison-shopping engines, optimize on search terms to help consumers do their searches effectively. They have hundreds of thousands of such terms they optimize on. And so for the purpose of a study, I've selected randomly 40,000 such terms, and these are examples of the kind of searches that we've done is among the 40,000.

Now, when you do searches like this, sometimes you'll get a comparison-shopping result, but sometimes you'll get a merchant in first place. Sometimes you'll get a content site. And so just to illustrate that point for the searches you show on the screen, you know, in rank one for this -- for Disney Winnie the Pooh, you get the Disney site and eventually get comparison-shopping. In this case, all of them are Google -- Google shopping.

Now, there's been some controversy here about whether Google provides these results based on an algorithm or whether they hard-

wired the results to favor themselves. And Google says, "Hey, we use an algorithm." And people like this Harvard professor, Ben Edelman, "Oh, they hard-wire the results to favor themselves."

But, to me, that's not the question. The question is, as the dominant supplier of search, are they running something that's neutral, fair to their competitors, and in the best interests of consumers? Is that what they're doing? Or are they providing manipulated results for their own benefit?

So when we started doing these 40,000 search analysis, we found some astounding things like -- you know, here's what came in, you know, first through AETH (ph) and our -- I'm using -- I mean, including merchants and everything else.

For the most part, Google came in -- Google shopping -- Google product shopping came in first place the most and it came in third place the second most. But, Google product shopping never came in second. Out of 40,000 trials, what kind of algorithm would generate that result...

(AUDIO GAP)

... when we took those seven examples, what we found is that every time Google was in second place, they were also in first place. So the result is they preferenced themselves an astronomical number of times. But, whatever system they're using can't possibly be a fair one because it doesn't produce a result that you would expect. How could they be -- never be in second place? So that seems to suggest there's something going on here that's just wrong.

Now, is it fair to competitors what they're doing? Well, I couldn't show this slide, but the result that we found is that as among these comparison-shopping engines, just as among the engines, if you just look at those, Google puts itself in first place 98 percent of the time, 98 percent of the time.

Even if I throw in a merchant, even if I throw in Amazon, the largest retailer on the web, Google still preferences itself more than 90 percent of the time. So the system they're running simply isn't fair -- isn't fair to Google's competitors.

What difference does that make? Well, this is the famous slide by Foundem, which shows that Google's share of product shopping was going down until they announced Universal Search and started preferencing their own stuff, at which point it started going through

the roof.

So, Google -- I can't -- OK, I'm not going to be able to get this one either. Let's see if I can get any of the others. OK.

Well, so --, the question then would be, does -- if Google is running something that's not fair to competitors, is it nevertheless fair to consumers? In other words, does -- yes, we'll get that in a second. Take that one off for a second, please? Can you get before that? No? Apparently not, OK. I don't know what the problem is here.

But, what I was going to show you is that maybe Google could say it's in first place 98 percent of the time because it provides the lowest price 98 percent of the time. But in point of fact, it does not.

And I was going to take as an example another one of these camera searches, and I was going to show you that in that preference box, Google has this camera for $2,000, whereas if you go to the sites below that they're selling the product for much cheaper than that. So the point is that by preferencing its own product Google is, in fact, hurting the consumer.

When shown this kind of information, the state of Texas, for example, said, "Geez, we've got to do an investigation. This is very serious. You know, we've got this whole sector of the economy. The results don't look neutral and straightforward. The results look like they hurt consumers. We've got to do an investigation."

The E.U. yesterday when shown in like this, this is a new study, but when shown information like this said, "We have got to -- we've got to make a formal investigation. We can't let this go forward without at least understanding what's going on."

But, of course, our government hasn't done anything, our federal government. Now, why is that? Can you bring me back up, the Mercimer (ph) slide, please? Why is it that our government hasn't done anything?

I don't know the answer. Could this be the answer? You know, this is a week before the election and the point person, the...

(AUDIO GAP)

... spokesperson for Google on this issue ...

(AUDIO GAP)

What are we supposed to think when we see something like that? You know, it is so troubling that we have to go to Europe to ask them to protect American consumers from manipulated search results. It's so disconcerting.

But, to see something like this, we just don't know what to think and we wonder what somebody in the Department of Justice would think.

OK, last point.

(AUDIO GAP)

(APPLAUSE)

SABO: Good morning -- or I guess, good afternoon.

There we go.

As stated earlier, I am here in my personal capacity. I'm not speaking on behalf of the agency or any particular commission or -- commissioner or any other staff member of the FTC.

But that said, as an antitrust enforcer, I'm also not here as a Google-basher, so I'll say that right out front. I -- you shouldn't assume that I necessarily agree with the comments or presentations made by the other panelists. As an antitrust enforcer, we have to be objective about all cases that come before us, and not pre-judge the facts. So, I'll start with that.

The FTC has, in fact, evaluated a couple of cases involving Google. Both of them have been in the merger context. In 2007, it was Google's purchase of DoubleClick and this past year their purchase of AdMob.

I was not involved in those investigations. I do conduct activity. So, we have several divisions that are merger shops that look at mergers. We also have a conduct shop and that's the one I lead. But, from what I understand about those matters and the lawyers who investigated them, there was, you know, a good basis for letting those deals go through.

When we look at merger cases as well, we're looking at all the evidence. We're looking at the documents. We're trying to figure out

if there's head-to-head competition between the companies at issue in the deal and whether or not letting that go forward would be anticompetitive or not.

And my understanding was there were very good documents in the Google-AdMob deal that suggested there wasn't head-to-head competition, and it was not a case that we would have been able to win had we challenged that merger. So -- and those cases, you know, involve market definition issues and other competition analysis.

Now, in the conduct realm, we follow a similar format. So, you have to determine what the market is anytime you're looking at a -- at an investigation. You have to figure out if there are new -- if there are entry barriers, if are there are new entrants likely to enter the market, and you also have to before you go forward with an investigation figure out if there's a viable theory of harm under which you can investigate the case or bring a case.

That's a legal issue, and we look carefully at -- I probably get a complaint a week that comes in from various folks on various matters, and the first thing we do is to see is there some theory of harm that would we could analyze that complaint under.

If we can, then we go forward with the next step and open an investigation and search for the facts and see if the facts actually support the theory of harm that we're -- or the various theories of harm that we're considering.

You have to analyze both procompetitive and anticompetitive effects. Will there be harm to the marketplace? And if so, are there legitimate reasons for why this conduct is occurring? And are there -- you know, are there justifications that can be offered by the complainant to see whether or not there really would be harm in the marketplace. So, that's how we -- that's sort of our basic format for how we analyze cases.

` When I think about Google, and as Gary said, I've given this presentation in another form in another forum, there are a couple of potential theories of harm that might -- that come to mind.

One is the changes in the search result and the algorithm that Gary spoke about significantly, and whether or not those search results would raise the costs of Google's rivals, raise their advertising costs, raise their development or operating costs or decrease the number of eyeballs that they see on their visitors to their sites.

A second theory of harm is information exchanges, and I'll talk about that in further detail. And then finally, are they -- a theory of harm of bundling or tying products together and whether or not that would impact advertisers. This is not a comprehensive list, but these are a couple of things that we think about when we think about Google.

And I won't discuss Foundem. I think there's been enough discussion about Foundem, but there have been a number of other complainants that have raised issues against Google. KinderStart filed a case in 2007, I think in the Northern District of California.

And what KinderStart did, as I understand, was -- had a website for parents of young children, so if they're looking for information about -- you're a new parent and you need information about how to get them to go to sleep or how to do this, that or the other, you could go to their website and get advice on these things.

KinderStart claimed that they were initially always at the top of the rankings if you looked for this sort of information. But then, overnight they dropped rankings by 80 percent. They lost 80 percent of their -- of the eyeballs on their site and were suddenly down at a very low rank, so similar to what Foundem experienced, as described by Gary.

They -- I think -- if I understand the complaint correctly, KinderStart didn't want to put a lot of ads on their site. They wanted to be an educational site for the visitors. They didn't want to have to promote advertising, and their view was that because they didn't host ads that Google then changed their ranking overnight.

They filed suit. They had claims in addition to antitrust, First Amendment and various tort claims like defamation and interference of prospective business advantage, and they were given the opportunity at least once to rewrite their complaint.

But, the court ultimately dismissed their antitrust claims saying that there were insufficient and conclusory allegations; that they failed to define a proper antitrust market. And they rejected one of the claims that Google was an essential facility and that they really needed to be hosted on Google. In part, the court rejected that claim because Yahoo! was out there and Bing, and the court said there were alternatives where KinderStart could get traffic.

TradeComet, I believe that was a case filed this year in federal court in New York.

(AUDIO GAP)

... re-file their case in another forum.

SABO: So, as to the first -- to the first issue about changing algorithms and how that affects your rankings, there are a couple of things we'd have to consider as an antitrust enforcer if we were looking at this, and this would apply to the FTC as well as DOJ.

What obligations does a search engine have to its rivals? And there was a Supreme Court case that was -- that came out a few years ago called Trinko. And the basis of Trinko is that there's no duty to one's rival. So, you -- as a competitor, you don't have an obligation to help your rival.

That would certainly be a defense that Google would raise if -- would raise, and that's something that an agency would have to contend with. Along these lines, we'd also look to see whether or not blacklisting really occurs. Google denies that they blacklist. They claim that they don't. They claim that their algorithm is objective. They say that they only -- they only prevent three things on their website.

They search for and look for pornographic sites and will block those. They search for malware, some malicious software and prevent that. And finally, they claim they also have a web master who looks for folks trying to game the system. So if you're hiring somebody to continue to hit on a site that would bring you further to the top, and they detect that, they'll try to prevent that.

So, any antitrust enforcer who wanted to look at this would have to look carefully into the allegations of blacklisting. And if -- what their rationale would be for doing that, and whether or not they do it or not are there less burden -- less burdensome alternatives that exist to get the same justification.

So, that's -- those are sort of the key questions that would have to be asked as to that first theory.

As to a second -- the second theory, information exchanges, these are where competing companies often share information, sometimes competitively sensitive information, in order to -- sometimes there are pro-competitive benefits and sometimes are nefarious benefits. So, information exchanges can be mischievous.

The concern is that if you're sharing online advertising information and you know that your competitor is bidding $3 to get on a site and you're bidding $2, and if that information becomes available through an information exchange, those prices tend to converge. And that's something the antitrust laws don't want to happen.

We want competitors competing against each other for pricing, not collaborating on pricing. And so, if there are information exchanges out there because companies have partnered and are sharing this information, is that a possible theory of harm?

If we looked at these, we'd -- we see that there are some situations. Google and AOL have a revenue-sharing agreement for Internet search advertising. There may be pro-competitive benefits for that, and there also may be nefarious reasons. And so, any antitrust enforcer looking at this would have to explore those issues. Information exchanges in this context would probably not be per-se illegal, but they'd come under what we call a "rule of reason," section 1 of the antitrust -- of the Sherman Act.

So, what possibly could be exchanged here? Bid prices, so a minimum bid prices, if those were shared, or if advertising prices were shared among these collaborations, that could be a problem.

And then it could be broader than just...

(AUDIO GAP)

SABO: ... of actual prices and being able to compare prices for the exact same keywords.

Now, there are pro-competitive reasons for information exchanges and they can, in fact, be done in an appropriate way. Over a decade ago, the FTC and DOJ collaborated on a safe harbor test in the health care guidelines. And these guidelines have been used throughout -- you know, beyond just health care to help competitors come up with a proper way of sharing information where it's necessary.

A safe harbor exists, and you would get the benefit of that safe harbor if a third party, an independent party, managed the information that was being exchanged.

If price data that was -- if it was price data being exchanged, it has to be at least three months old. So, it can't be current price information. You have to have at least five participants in the

exchange, and the theory there is if there are -- the more people exchanging, the less you'd be able to identify whose prices were -- belonged to who; and finally that the data be aggregated sufficiently so that it would be anonymous.

And that's -- if you followed all those steps, as a -- you know, as a company involving -- involved in an exchange, you would get the benefit of the safe harbor under these guidelines.

So, again, if an investigation were to launch on Google under this theory, we'd be looking to see if there were legitimate efficiencies realized by partnerships and vertical relationships, whether they could be designed in a manner that didn't run afoul the antitrust laws and, you know, whether an -- a Chinese wall could be implemented if necessary.

And finally, another theory of harm is raising rivals' costs and bundling. Foundem raised these in comments to the FCC, as well as a New York Times opinion piece that I think they did the end of last year.

Their claim is that Google, as has been discussed already, gives preferential placement to its own vertical search engines, such as its price comparison site. And in the future, they could start expanding that to other...

(AUDIO GAP)
SABO: ... sites, so Google Travel...

(AUDIO GAP)

SABO: ... but they give deeper coverage of one topic so travel, price, maps, videos.

They're ad supported. Some of...

(AUDIO GAP)

SABO: ... or if you wanted to use Google, you could put Foundem in that and it would pull it up. So, they're not preventing you from getting to those sites if you want to see them.

And others...

(AUDIO GAP)

SABO: You know, another issue is Google...

(AUDIO GAP)

SABO: ... in acquiring -- acquiring companies like ITA, which is -- I believe is still under review by the Justice Department. They acquired YouTube, and they've grown organically as well.

But that said, competitors are also vertically integrating, and looking at what competitors are doing is a significant part of any investigation.

This is an example -- just an example of vertical search and the various ads and unaffiliated conduct that would come up.

So, again, if we looked at -- if we looked at this theory of harm, and this is one I will say -- raising rivals' costs and exclusivity is something that we do a lot of. Half my docket is probably looking at those kind of cases right now.

But, integration -- integration can be good. It can give you relevant information. It can organize the site for, you know, for the viewer. It can create and improve services, so there could be potential efficiencies and good things about integrating vertical search.

But, again, there could be potential anticompetitive effects as well, as I said, excluding rivals in foreclosure, allowing firms to bundle related advertising services can prevent -- you know, prevent you from getting to the site, preventing you to get advertising dollars if you're a competitor of Google.

So in closing, the agency will continue to monitor this, review any proposed mergers carefully that come through, and wait and see what happens in terms of whether or not an investigation opens.

I should mention, we collaborate -- both Justice and the FTC collaborate regularly with the European Commission. Most recently -- my most recent example is Intel. In that case, the E.U. was out in front of the FTC, but that didn't stop us from bringing a case.

And on our Rambus matter, we were out in front and then assisted the E.C. with their Rambus case afterwards. Justice collaborated with Microsoft -- with the E.C. on Microsoft.

So, the fact that the E.C. has announced this case investigation

first doesn't -- isn't -- I would say isn't extraordinary or isn't unusual. They -- and you may well see something soon from the U.S. agencies, but I can't promise anything there.

(UNKNOWN): Go ahead and promise.

Thank you, very much, Melanie.

(UNKNOWN): Thank you.

(UNKNOWN): I think we're at a -- why don't we just go right to questions from the floor? And please identify yourself. Yes? Identify yourself and your affiliation when you pose the question, please.

FILLMAN (ph): Ross Fillman (ph), I'm with the Computer and Communications Industry Association.

(UNKNOWN): Thank you.

FILLMAN (ph): And I guess my -- you know, just hearing all this, my biggest question would be how -- what would you -- how would you fix this? And what would Google or Bing or anyone else who's kind of coming over -- under a similar scrutiny, what do they do to fix this that doesn't break search?

I mean, I think an easy answer is, well, you know, let us see the algorithm and then we can all see whether or not -- but I mean, obviously that games -- that gives everyone the ability to just game the system and search becomes unusable.

REBACK (?): Yes. So, it's a very fair question. Of course, it's hard to know what the right remedy is without doing an investigation. I mean, that's why you do an investigation.

But, let me give you one scenario which has worked in the past, which is this committee of technical experts that oversees the Microsoft settlement that's been going on now for five years.

You know, you point out that we wouldn't want a search engine company to disclose its algorithm publicly, and I'm sure that's true. But with respect to Microsoft, because they were held to be in violation of the law, they had to disclose source code to the technical committee so that the technical committee could see whether they were behaving appropriately or not. It turns out that they were.

So in this case, you could certainly do exactly the same thing and have the technical committee look at the algorithm and see whether it's biased against competitors without, as you say, eliminating spam and malware and stuff like that.

Now, will that work? I mean, I didn't think it work in Microsoft, and it turned -- I'm going to have to admit I was wrong. It turned out to work. Would it work here? It's certainly a start, and we know we have a way to make it -- that it's worked before. So that's where I'd start. I'd try that. If that doesn't work, then we'll try something else.

We just can't leave this in a situation where it's going. We've got to do something about it, and the right start to that is to conduct an investigation and try to look carefully at the kind of questions you're asking. That's my view.

(UNKNOWN): Melanie?

SABO: Well, I -- you know, I -- I'd have to say we didn't use that route on Intel. We didn't go to a technical committee. There are those who think that actually that was 20 years later or 10 years later than the Microsoft matter. It's -- I think if you ask the Justice Department, they'd say that was a nightmare.

So, I -- we didn't elect it in Intel. That's all I'd say. We didn't elect going that route in Intel. But one would have to look carefully at what the remedy would be, and I can't speculate as to what that would be now.

(UNKNOWN): Other questions? All the way in the back?

BRADY (ph): Hi. It's Betsy Brady (ph) with Microsoft.

I'm just curious about what you all think that the Europeans are doing in their move. I mean, there's just a lot of conjecture about where they're focusing. They've got a couple of companies they're looking at, but now they've broadened the investigation. And I don't...

(AUDIO GAP)

BRADY (ph): ... know if anybody has any greater insights, given the...

(AUDIO GAP)

(UNKNOWN): ... issues, so I think it's very sweeping. I think most people understand when the E.U. starts diving into this arena, they tend to be serious. So I think it's the single, most ominous antitrust development for Google yet.

And I think it's a very serious, very, you know, threat to Google, and I would be surprised if they wouldn't admit behind closed doors that of all the things that happened in the antitrust arena, this is the most ominous and troubling.

(UNKNOWN): I guess one thing I would add, of course, none of us know. Those -- their deliberations are confidential, just as FTC and Department of Justice. Google's share -- Google's reported share of search in Europe exceeds 95 percent in most countries. I don't know if any country it's lower than 95 percent.

And their standard for -- their antitrust situation is a little bit clearer. We have all this case law that's all mooshed up and the Sherman Act and all these other things, and they have a very straightforward standard, which is if you're a dominant company, you can't use that dominance to distort competition. That's really it, and that's the basis on which they went after Microsoft and the basis on which they've gone after other companies.

The one thing that I would add, last thing, is that the Europeans started with these complaints from three companies in Europe. They've gathered a lot more information than that, and they've gathered information including from American companies.

So, I don't think -- I'm relatively certain this is not a step...

(AUDIO GAP)

(UNKNOWN): ... they've made -- drawn any conclusions at this stage. They're doing, I think, what they should do. They're taking a formal look.

(UNKNOWN): A question over here on the right?

MANISHIN (ph): Hi. I'm Glenn Manishin (ph) from Duane Morris.

(UNKNOWN): I think you should add probably that you represent Google. Is that correct?

MANISHIN (ph): I do not represent Google.

(UNKNOWN): Oh, I was given to understand that your firm did.

MANISHIN (ph): No. My firm does not represent Google. I don't represent Google. I'm not being paid by Google.

(UNKNOWN): That's fine.

MANISHIN (ph): Thank you, for...

(UNKNOWN): Thank you.

MANISHIN (ph): ... clarifying that.

My question goes to the assumption that you two gentlemen started with. If the point of search is to provide predictive results that consumers find useful, how is it possible that anyone -- how is it possible that any search engine, whether they have share or not, could be required to adhere to a standard of neutrality, since the point of search is not to deliver neutral results, but rather results that are predicted to be most useful to the consumer making the search?

(UNKNOWN): I think that's a variation of a lot of defenses I've heard from Google, and it's basically a circular argument. It's clever, but it's basically like saying that, you know, there's no way that we could do anything anticompetitive because the business we're in is naturally focused on users and delivering results that they have.

And it -- what it -- it's circular logic, and it's also very clever in taking a tunnel-vision view that says that there is nothing else that someone could do outside of that narrow tunnel frame that could be anticompetitive that could have an impact on that statement.

So I think it's a clever public frame to say, you know, it couldn't be anticompetitive by definition, and Google generally does that. It says, "Look, everything we do is because we love users. And antitrust law is about protecting users, and we protect users, so we never could by definition violate antitrust."

They have made their defense of antitrust tautological, meaning that whatever they do is inherently pro-competitive because they've justified it by pro-user and pro-innovation.

(UNKNOWN): Well, I guess I tried to go through this in my presentation. I think this is -- I mean Google would like to debate

the point about whether search can be neutral or not. But that's not the contention that certainly people on my side of the table have in mind.

As a dominant company, is Google Search fair to competitors? That's one question. I think the answer to that is no.

The second question that the -- that you allude to are: Are these results in the best interests of consumers? When they preference their own stuff, are consumers getting the best information? Are they getting the lower price?

Well, we've done this big study. They're not getting the lower price, and they're not getting the lower price in the top positions because Google is preferencing its own properties.

So those are the questions. I don't think anybody's going to debate the issue of whether search needs to be neutral or not. This is -- the question is whether Google's conduct is abusive in terms of competition policy or not. That's the question.

(UNKNOWN): Melanie, anything to add to that?

SABO: Again, without doing a full investigation, I wouldn't comment.

(UNKNOWN): Thank you.

(UNKNOWN): I think it's probably about time that we all headed over towards the tables and helped ourselves to lunch. And then, we'll be joined by Daniel Weitzner from the Department of Commerce to talk about their pending privacy report. So I thank the panel very much, and please enjoy the lunch.

(APPLAUSE)

(RECESS)
SIMPSON: Well, welcome back after that brief lunch. Again, I'm John Simpson, director of Consumer Watchdog's Inside Google Project. We are webcasting this, so welcome to those of you on the web who are watching.

It is a live webcast now. Tomorrow, the whole thing should be available to the same URL, and you can call it up. Probably later in the week, we'll have it broken down on our own website by specific panels to make it a little easier to find things.

So right now, I was just...

(AUDIO GAP)

WEITZNER: ... think I should probably go do something else, because I've been doing this excessively long. And I should start by saying, congratulations to our colleagues at the Federal Trade Commission. I'm sure someone's out there on the webcast. It's a terrific thing that their report is out.

As John said, I think it's a very exciting week for those who care about privacy. Between the FTC report, this event, there's an event later next door. We have Chairman Rush's privacy hearing tomorrow, and I can promise you that very shortly you'll also be able to see the Commerce Department's privacy green paper. But there's no doubt that the FTC contribution is going to be very important in shaping the administration's view on where we go on privacy policy.

I'm really, really happy to have the opportunity to talk with all of you, and I appreciate...

(AUDIO GAP)

WEITZER: ... Consumer Watchdog's...

(AUDIO GAP)

WEITZNER: ... sense with the recognition of just how important the Internet was in the 2008 campaign in bringing the kind of climate that brought President Obama to the White House. So for us, privacy protection is really a key part of preserving the open Internet environment.

Fulfilling this promise is a key goal of the Interest Policy Task Force that was created by Secretary of Commerce Gary Locke this April. The department is engaged in a broad review of four key public policy challenges facing the Internet: number one, enhancing privacy; number two, ensuring cyber security; number three, balanced copyright protection; and number four, ensuring the global free flow of information.

That last one is our -- is the Commerce Department's complement to the State Department's Internet Freedom Initiative. Our decision to address this range of issues arises from the significant and growing social and economic contributions that the Internet makes in

all of our lives.
According the U.S. census, domestic online transactions are currently estimated at a total of $3.5 trillion annually, and that number will go up obviously substantially.

Digital commerce is a major source of job growth as well. The new study looked at the period between 1998 and 2008 and found that the number of domestic I.T. jobs grew by 26 percent in that period, four times faster than the U.S. employment growth rate overall.

By 2018, I.T. employment is expected to grow by another 22 percent, so this is clearly an area of the economy that's critical. And from our perspective, it's critical to address privacy questions to create a trusted environment in this new economy.

Privacy was the Internet -- is the Internet Policy Task Force's first order of business. Our effort is guided by two over-arching policy principles. First, preserving consumer trust is essential to the sustainability and continued growth of the digital economy.

If users do not trust that their personal information is safe from misuse, they will worry about using the next new Internet-based services and thus threaten the economic growth and innovation that we're all so dependent on.

Second, Internet policy implicates a broad array of interests -- industry, consumers, civil society, academic and governmental interests, and we need a policy development process that includes all of these stakeholders. And that's why I'm especially glad to be able to be at an event like this.

We must learn from the unique multi-stakeholder processes that have helped build and operate the Internet today in order to arrive at best practices that can protect user privacy according to a flexible, but enforceable set of rules.

In the years following the commercialization of the Internet starting in the mid-90s, an era that we tend to call Internet policy 1.0, the government imperative was to seek unrestrained growth in the Internet as a promising new medium.

During this first phase of Internet policymaking, early online privacy engagements between the Commerce Department, the FTC and commercial and noncommercial stakeholders collaborated to establish a model for addressing emerging privacy challenges.

These efforts led to progress towards voluntary enforceable codes of conduct and opt-out opportunities. The premise of this effort was that voluntary industry commitments would develop faster and provide more flexibility than legislation or regulation.

The Internet grew rapidly through the next decade, the 2000s, and supported tremendous economic growth and social innovation. Personal data available on the Internet also grew rapidly in volume and granularity, which in turn expanded the market for personal information.
During this era, which we call Internet policy 2.0, Congress acted on discrete challenges such as combating spam and protecting children's personal information. Meanwhile, the over-arching notice and choice model of privacy policy remained basically unchanged.

The FTC, of course, continued to enforce companies' obligations under this framework, but the previous administration ceased its promotion of industry codes that would have addressed new privacy challenges.

Today, we face many of those challenges in the third decade of Internet policymaking. There's little question that multi-stakeholder organizations have played a major role in the design and operation of the technical aspects of the Internet and are very much responsible for its success.

Our approach, which we call Internet policy 3.0, recognizes that the interplay between amongst technical standards and design, multi-stakeholder institutions, voluntary best practices, and laws and regulations is essential to ensure that the Internet continues to meet its economic and social potential.

But has this current model really worked well enough in the privacy arena? Should we continue -- should we consider continued reliance on it? As experienced web users, we all know that few people read privacy policies. Even if you try, the language is usually disappointingly vague and confusing.

If most Internet web users don't actually read and make choices based on these posted policies, then are these policies really delivering the transparency that our reliance on the Internet requires?

Would it have been preferable for us to engage in a different policy approach during the early days of the Internet such as having Congress or the FTC enact a set of fixed substantive privacy rules for

web companies to follow?

We think the answer is no. The focus on transparency during the privacy debates in the 90s was to enable the development of a system in which advocates, regulators, companies and their customers were able to engage in a dialogue about what constitutes acceptable privacy practice as measured by evolving consumer expectations.

As privacy scholars, Professors Deirdre Mulligan and Ken Bamberger from the University of California, Berkeley Information School and Law School, respectively, recently wrote, "This type of dynamic hybrid system in which both private and public stakeholders participate may well yield actual privacy practices that are more responsive to evolving consumer expectations than would a traditional rulemaking system."

The rate at which these new services develop and the pace at which users form expectations about acceptable and unacceptable uses of personal information is measured in weeks or months. We all know that rulemaking at agencies such as the FTC or the FCC can take years and could result in rules addressing services that have long been abandoned.

But at the same time, in response to the Commerce Department's privacy in innovation notice of inquiry that we released in April, a wide range of commenters from both industry and civil society told us that the current privacy environment must be strengthened, that it's not doing the job.

In other words, we need to build on the innovation-promoting strength of our current model, while at the same time increasing consumer trust.

So what specifically done -- needs to be done to strike this new balance?

First, we feel that it's time to commit to a baseline set of privacy principles. To borrow from one of the responses we...

(AUDIO GAP)

WEITZNER: ... we received to our (inaudible) across the many commercial contexts in which personal data is used.

We need to investigate the appropriate safety net for when the marketplace fails to meet consumer expectations tied to these baseline

FIPS (ph)

Second, with our multi-stakeholder model, we realize that government is not going to have all the answers. A multi-stakeholder strategy for implementation will be critical to ensure that we end up with a framework that is rational and provides businesses with a clear set of markers about how to meet their obligations, but is also dynamic to keep information practices in line with consumer expectations and evolving business...

(AUDIO GAP)

WEITZNER: ... broader focus on data privacy. So I'd like to mention how we relate to this effort -- we -- how we relate in this effort to other agencies.

About a month ago, the White House announced the formation of a privacy and Internet policy subcommittee to further advise the Obama administration on Internet privacy policy.

This subcommittee, which Commerce Department General Counsel Cameron Kerry co-chairs with Assistant Attorney General Chris Schrader, is working to coordinate federal agencies in an effort to promote a broad, visible, forward-looking commitment to a set of Internet...

(AUDIO GAP)

WEITZNER: ... the area that's related to do not -- the do-not-track concept is intended to address in the area of online behavioral advertising and other advertising mechanisms on the Internet going back some time.
As web users became aware that cookies could be used to track their activities on a single website, as well as across multiple websites, browser developers provided their users with means to block and manage cookies in a variety of ways.

Most recently, members of the online advertising industry developed common principles about the collection and use of this tracking information, and the industry is rolling out a system to help consumers manage their tracking preferences online.

To the extent that these tools provide effective protection for individual choices, government properly avoids regulations that would otherwise restrict the flow of information.

Any do-not-track system would necessarily have two components: first, a technical mechanism most likely built into web browsers that provides the user a way to signal his or her intent not to be tracked or profiled, depending on the context; and second, an understanding between those individual web users and all of the various commercial and noncommercial services on the web that engage in tracking as to exactly what sort of behavior those services would avoid.

The technical mechanism may take some time to implement, but it's a relatively straightforward engineering task.

The second part of the task, figuring out what that do-not-track, do-not-profile, do-not-advertising signal actually means and who actually is obliged to respond to it, is I think a much more complicated task requiring agreement on policy, best practices and best practices among a number of players, including users, advertisers, marketers, technology companies and other Internet intermediaries.

Some users want to avoid tracking altogether. That is, they want to be sure that no website or third-party service collects or stores any data about their web-browsing behavior. That goal can largely be accomplished with existing browser settings and additional tools that are coming onto the marketplace for unilateral action by users.

For these users, greater consumer education about the tools available may well be needed. But many users want a more nuanced set of choices, and I think we all recognize that. That is, users might be happy to have certain sites collect and store information about their browsing habits when it serves the user's interest, but they might want to avoid other tracking or profiling that they consider intrusive or simply of no benefit to them at all.

In the first instance, a user may want sites to remember his or her preferences, account information, or even provide certain types of customization. However, that same user might also want to prevent the creation and use of profiles that allow marketers or advertisers to learn details about his or her buying habits.

Reaching agreement on this more complex set of choices beyond just the technology mechanism is going to require careful work. So today's debate about the feasibility of do-not-track is an illustration of a larger problem: the over-arching need for a more dynamic framework that can incentivize the creation of industry codes of conduct and associated technologies, while also being flexible to keep up with the pace of innovation.

The robust, dynamic framework to be proposed by the Commerce Department's green paper will provide increased ways to address new applications and technologies such as those I think hoped for by some of the do-not-track discussions.

Specifically, the Commerce Department's Internet Policy Task Force will look for opportunities to convene industry and consumer groups to reach voluntary agreements on issues such as affording users better ways to control the flow of personal information and to signal these choices to companies online.

Our department's task force is also well situated to work collaboratively with the Federal Trade Commission to encourage industry to create workable models in these and other areas. Once crafted and adopted by the range of commercial and noncommercial stakeholders, the FTC can use its enforcement authority to ensure compliance with these voluntary agreements.

In closing, I'd like to say just a few words about the roles of various stakeholders in the privacy debate -- users, consumers, privacy advocates, businesses and the Federal Trade Commission.

Users, we think that you are right to expect a web experience that enables you to exercise meaningful control over how your personal information is collected and whether third parties are using your information in a manner that is inconsistent with your expectations.

Privacy and consumer advocates, I believe very personally that the web is and hopefully will continue to be a work that's very much in progress. So your voice, your role as a voice for consumer interests is critical to technology design and technical standards bodies such as the Internet Engineering Task Force and the Worldwide Web Consortium.

It's important to be represented in the public policy debate, of course, but the user voice is represented by consumer advocates. It's vital in the process of shaping the global Internet technology environment on which we all depend.

To businesses and telecommunications companies, you've been extraordinarily innovative in developing new products and services that add value to the online economy through increasingly creative uses of personal information.

Various individuals and companies, industry groups are now

applying that innovative spirit to tools that give users transparency and control over their personal information, which they very much deserve. And we hope you'll keep that coming.

Finally, the -- to the Federal Trade Commission, the Commerce Department, there's not a whole lot I can say about what's in our report. But, one thing I can say about what's in our report is that it will -- the framework that we will lay out will depend critically on the continued role and the groundbreaking work that the Federal Trade Commission has played over the last 15 years in online privacy protection, beginning when the web was young and growing with it as it has expanded.

Some countries express worry about the lack of privacy protection in the United States. I think that what they sometimes don't take account for -- what they sometimes don't take account of is the really extraordinary role that the Federal Trade Commission plays as a critical, if not the most successful, consumer and privacy protection enforcement agency that we see all around the world.

I want to just paraphrase in closing a set of remarks that Peter Hustinx made at the International Data Protection Commissioners and Privacy Commissioners Conference in Jerusalem last month -- or in October, rather. Peter Hustinx is the European Union data protection superintendent. He's responsible to the parliament to develop recommendations for reshaping the European Union data protection directive.

And in remarks that he made on stage he gave a kind of a thumbnail...-.

(AUDIO GAP)

WEITZNER: ... and he said, "Now, we have things to learn from each other." And I really couldn't agree more with Mr. Hustinx. And note that when he refers to implementation, what he's really talking about is the two key pillars that we've had in U.S. privacy policy, U.S. commercial data, privacy policy today: the development of voluntary, enforceable codes of conduct by -- in the private sector and the extraordinary enforcement in policy work of the Federal Trade Commission.

So the Commerce Department looks forward to working with all of you, all of these stakeholder groups, as we continue to develop new tools, new best practices and evolving social consensus about how to handle personal information online.

Our challenge, we believe, is to create a framework that enlarges U.S. prosperity and democratic values while providing meaningful tools to empower individuals to make informed, intelligent choices for protecting their privacy.

Thanks very much, and subject to my colleague, Moira (ph), I have time for a question or two, I hope. One, she says.

(CROSSTALK)

(UNKNOWN): (inaudible) multiple part. I just -- I don't quite understand your -- what you're saying about do-not-track. You said that basically the browser settings are enough to limit tracking.

And I guess I just want to point out that we at The Wall Street Journal have been writing a lot about all these advanced tracking techniques that really aren't blocked by the browser.
So, I just wanted to see if you could clarify a little bit about what it meant.

WEITZNER: Well, I think I talked about browser settings and then other tools that users can use. Those are -- those though, I would stress, are blunt instruments. There are mechanisms by which users can travel around the web with some degree of obscurity, not perfect, but with a fair degree of obscurity.

I think the main point I would make is that it seems unlikely from the evidence of the online marketplace that most users actually want such blunt instruments. What users seem to want is more fine-grained control.

(UNKNOWN): OK. So does that mean that in general you guys are supportive of do-not-track?

WEITZNER: I would say that we are very supportive of what we said, which is we're supportive of tools that give users more control about how their personal information is used and how they're involved in profiling and targeting activities.

(UNKNOWN): One more?

WEITZNER: Go ahead.

(UNKNOWN): And then finally, you talked about -- you were vague about whether legislation is needed for some of these things to

happen. Can you say whether you think it is?

WEITZNER: Well, let me just say the role that we hope our report will play. We think our report is important in taking a first -- to enable the administration to take a first concrete step into the privacy policy dialogue. And what we will hear back from our report will help it form administration position on legislation in the end.

It's not up to the Commerce Department to decide what position the administration as a whole takes on legislation. Our job is to provide the best background, to collect the broadest range of views that we can towards reaching that position. And I think that's going to be...

(UNKNOWN): Can you take one more -- one more?

WEITZNER: I think I've got to go, but I'll be happy to talk with you afterwards.

John, thanks very much, really appreciate it.

SIMPSON: Well, I'd like to call the next panel up if we're ready. We're trying to keep the trains moving, as they say. And I always was a frustrated train conductor, so -- we seem to be having some success today at keeping things on time.

I think -- we'll just all speak from up -- right here, I think. I do this in front of every panel just because, ultimately, I think some of this may be archived separately on the web by different things and so on and so forth.

So those of you who already know it, I am still John Simpson, director of Consumer Watchdog's Inside Google Project. And this panel initially was thought of being about many of the ways that the Internet affects some of the creative arts, and we had anticipated having some additional folks join us, coming from other areas perhaps than the literary world.

But I kind of am of the view that all real important art flows from the literary world, and so it's entirely appropriate to have this panel. And we may get into some other areas beyond that sort of impact.

We're going to just sort of -- I think we'll just go down the panel in five- or seven-minute opening statements and then maybe a little interaction here. And then we'll open it up to questions.

And I'll introduce everyone right now. Stuart Bernstein is all the way down at the end. He's an independent literary agent based in New York City, former bookseller. He founded his agency, Stuart Bernstein Representation for Artists, in 1995; works with writers of literary friction -- excuse me, fiction and nonfiction in all categories. He has been, I might add, an outspoken critic of the Google Books settlement.

Next to me is Michael Capobianco, who is co-author with William Barton of four science fiction novels and the sole of author of one. He served as president of Science Fiction and Fantasy Writers of America from '96 to '98, 2007 to 2008. As a long-time observer of the digital publishing scene, he acts as the point man for the science fiction writers on the Google Books settlement.

Sally Shannon is a freelance writer and the current president of the American Society of Journalists and Authors, which represents the nation's independent nonfiction writers, whether their work appears in books, magazines or online.

She had been president for five years when she read the originally proposed version of the Google Books settlement and one night after dinner became outraged at perceived violations of copyright and antitrust law buried in its pages.

Some of you may think that we perhaps have tipped some of these presentations to be slightly in opposition to Google. I wanted to just reiterate that we have repeatedly invited them to be on any panel that they chose to be on. And in fact, if there's anyone here remotely associated with Google at any time who wants to ask a question or make a point, we encourage them to do so.

In more than 20 years as a freelance writer, Sally also had assignments from major circulation magazines. She's for Women's Day, Reader's Digest, Parents, Good Housekeeping, Savior (ph), Smithsonian and more and more and more.

So we're honored to have this panel, and Michael, why don't we just lead off with you if you don't mind?

CAPOBIANCO: OK. As John said, my name is Michael Capobianco. I am a past president of the Science Fiction and Fantasy Writers of America, and I act as their point person for the Google settlement.

Science Fiction and Fantasy Writers of America was formed in 1965. It's a nonprofit that's dedicated to author advocacy, primarily

for science fiction and fantasy writers. We also promote the best in the genre by giving the Nebula Awards every year. So, we have a -- kind of a multi-tasking purpose there.

We came out in opposition to the Google Books settlement, and I might be able to get into more about that later, but I won't pile on at the moment with Google attacks.

Part of the title of this panel involves how is the Internet treating creative writers and creative people of all sorts. And as usual, with a complicated question like that, Dickens is the appropriate quote, which is, "It was the best of times, and it was the worst of times."

It's the best of times for a creator if he or she wants to have their work disseminated in a wide way without any intermediaries, without anybody telling them what can be in it or what cannot be in it. It's very simple for someone to create a web page or a Facebook identity and reach thousands of people overnight with anything and everything they choose to create.

On the other hand, it's the worst of times if you want to get paid. And for many creative people, that is a consideration. Most of them, or many of them, if they cannot earn a living or earn money from their creative works must work another job.

Some of them aren't suited to do anything but write, and they end up working at McDonald's because basically creative people are creative. They're not necessarily those who can work in an office environment, you know, you never know.

I did want to say that listening to the other presentations and thinking about how this panel fits in, it's interesting that in a way what we're talking about for -- what we're advocating for on the Internet is basically copyright, some reasonable version of copyright.

And it doesn't have to -- probably, you know, the current copyright laws probably go too long, and there are probably other problems with them that could be worked out in the framework of a digital environment that would be fair and would work better.

But as long as the Internet is a place where people can be essentially anonymous and can violate laws at will, and primarily copyright laws by trading information, by trading books, by trading music, you have a situation where you have virtual crime. And virtual crime is not being pursued in any sense. It's just -- there's no way

to control it.

We feel that the Internet will be best, will work to its best and highest potential if creators have control over the distribution of their works. And to that end, we think that we have to have a system in which creators have a say in how things are done.

I'm not a lawyer. Most of my fellow writers aren't lawyers, except for John Grisham, people like him. And so, we're kind of at a loss to how to react to the current situation. Creators tend not to be public people. They tend not to be up on all the legal niceties of copyright.

So basically what -- I guess I'll end by saying that what we want to see is a system where consumers benefit and copyright stays something that is available for writers who choose to use it. Some writers might not, and we'd like to see the Internet develop in that way.

SIMPSON: Sally?

SHANNON: Thank you. I want to correct one little thing that John said initially. I had been president of ASJ for five weeks when I realized that I really needed to read that voluminous Google Books settlement and find out what was in it and stop relying on what my friend, the executive director of the Author's Guild, of which I also am a member incidentally, was telling me.

And I read it and was astonished, just astonished, and then outraged at the way everything runs to Google and to the publishers and against the creative people who give us our books and our blogs and our magazine articles.

In 2005, when we all first heard that Google was going to produce what it called the world's largest Internet library, a huge -- likened to the Library of Alexandria, where any child anywhere in the world could turn on a computer and tap into the world's greatest books, we were I think all a little bit torn, those of us who write for a living.

First of all, as readers, how can you not think "fabulous." Who wouldn't want to have a tool like that for research and for your own reading pleasure? On the other hand, Google was copying our books without asking our permission. It was wholesale violating copyright and made it perfectly clear that it intended to continue doing so.

Well, you know basically the story. The (inaudible), a fabulous online library, and then the Author's Guild sued Google. The publishers filed a similar suit. The court joined the two suits together.

They went into settlement talks for four years, and at the conclusion of those settlement talks, instead of coming out with the world's largest, most fabulous library, they came out with the world's largest book store.

In other words, the settlement set up Google as the seller of digital books, in competition with Amazon primarily. Clearly, they were targeting Amazon. So we were deceived in that sense, all of us, not just writers, but all of us consumers -- deceived.

A lot of times you hear that the Google Books settlement, if it comes to pass the way it's currently structured, and of course the court is now considering that second attempt at getting it right, that you hear it likened to ASCAP, the modality through which writers of songs get paid for their music when someone uses it.

Well, it's an incorrect analogy because, first and last, ASCAP has never been something that songwriters were compelled to join. It has always been something that proved itself. It came into being perhaps 40 years ago, and songwriters had the choice whether or not they wanted to be paid through ASCAP.

At first, only perhaps 9 percent or 10 percent joined up, but then ASCAP proved its worth and more and more people did. Of course, ASCAP also operates under the supervision of a court because it's been sued for violation of antitrust...

(AUDIO GAP)

SHANNON: ... settlement if all the books beyond a certain date, a fairly recent date, are in the Google Books settlement like it or not.

Now, writers theoretically were given the attempt to opt out, but a great many people never knew about it. And as Michael said, creative people tend not to be tremendously in touch with things legal or things of copyright.

And I think -- you here are writers and reporters. You know copyright issues make our eyes glaze over. Don't they? I mean, who wants to spend our time writing about copyright or knowing about it?

Yet, friends, our livelihood depends on copyright law. If we don't control what we write, then how can we make a living? And that's the center of the question of the Google Books settlement for us.

I could say a lot more. I could give you a list with 17 reasons writers should hate the Google Books settlement, or reasons that every consumer should be very, very leery of it, but I'll stop for now.

SIMPSON: Stuart?

BERNSTEIN: I thought -- I kind of predicted that my colleagues here would be talking a lot about copyright, and as a literary agent I thought I would maybe just give a little history of book-selling because -- as I've seen it over the years.

I started out as a book clerk in the late 70s in the Scribner bookstore, which was a bookstore with a publishing house upstairs. And Charles Scribner used to come down and visit with us down in the bookstore.

As things have changed over the years, first there was a moment of the chain stores coming in and knocking out the smaller bookstores. And I think that what's happening with Internet book-selling, with Amazon, with Google, with Apple, is really just a next step, with the Internet mixed in, of this corporatization and consolidation of book-selling, which is -- it's not really a good time for writers unless you are already a very big name, very well-known writer. And I think there's a history of publishers capitulating to the latest retailer on the block, giving -- in the late 80s and 90s, giving favorable terms to the big chains and now basically doing whatever Amazon tells them they need them to do.

I have -- there are certain features of shopping for books on Amazon that we all know, like looking inside the book, being able to search through a book. I represent writers who really care about the words that they put down on the page, and there's a certain kind of sloppiness to allowing the consumer to search through a book.

And what they're telling you is that this is going to entice people to buy the book. Why not come up with just this nice static sample chosen, a cliffhanger, a teaser? That's the way it used to be done. That's the way some medium and smaller publishing companies are still doing it.

So, there's -- basically, you're allowing people to look inside a book. You can look at 20 percent of a book within a 30-day period.

After 30 days, you can look at another 20 percent of that book, and these kinds of programs are just not being done with a lot of thought.

The big book sellers who are -- are going to be the only book sellers very soon, are not concerned with the interests of the creative person. There's lots of creativity on the Internet and I'm definitely someone who enjoys it. And it enables writers to connect directly with readers in ways that they never could before.

But writing, especially the long-form narrative, whether it's fiction or nonfiction, depends on reflection. It depends on someone having an attention span that allows them to sit down and read an entire book. And what we have now is the Internet basically is an interruption of that -- that attention span.

So, I understand that the -- when Google puts their bookstore up, a book is not going to be listed there unless you make it searchable in the way that Google wants you to.

There's a whole complicated underbelly to the book business that -- that these people don't understand. They are not book people. Amazon, when it was first set up, it was a business designed to sell something.

And Jeff Bezos had a list of things that he could possibly sell and books seemed to work well for the -- the scheme of gaining market share, of becoming a destination for eyes.

I find it very frustrating that publishers are just basically laying down. They've -- they've, over the years, just destroyed the structure of what helps sell books, so that no longer are they taking risks on new young authors. No longer are they letting an author publish two or three books before they catch on.

There are authors like Ian McEwan who had a great big hit after I think it was four or five, six books. It's -- it's not going to happen anymore. New voices are not going to come out. There's no serendipity in shopping online the way there is walking into a bookstore. Those bookstores are -- are just simply disappearing.

So, it's -- I -- I find it -- it very -- a very frustrating time and it's a transitionary time and there are going to be new ideas and new ways to -- to sell books and to control it yourself. But you're forcing authors into a position where they're no longer able to just -- just think about their work. They have to think about selling. They have to think about communicating. They have to think about

blogging.

They have to think about all of these things that was never their job before. And by capitulating to these big -- big steamrolling Internet companies -- Amazon, Google, and even Apple -- and narrowing down the -- the -- the books that are -- that can be sold or that can be sold successfully through those channels, the publishers are -- are going to capitulate themselves out of existence, which is going possibly be a good thing.

Possibly be a -- a -- just a terrible, terrible thing because if they narrow themselves down to just the big-name authors and just selling the big name authors, those are the people who can go out and do it themselves. Those are the people who can hire a copy editor, hire somebody to design their book, and hire somebody to -- to put it on the Internet for them and sell it directly to the consumer, and then there'll be absolutely nothing -- nothing left.

In any case, by creating a universe where only the popular survive, for writers, it's -- there's -- there doesn't seem to be too much -- too much of a -- of a future.

SIMPSON: Thank you.

Well, let me just ask a question or two and, then, we'll go to the audience for questions.

Michael, you said something -- you touched on something that I'd like to have you expand on it a little bit. You said that, well, I understood you to say that you didn't think the Internet could really function successfully unless -- unless we've got a way with -- unless we stopped anonymity. What do you mean by that?

CAPOBIANCA: Well, OK. As I understand it, now I'm not a computer programmer either. But basically there are many ways for a user of the Internet to avoid having themselves identifiable.

Either they can use -- they can spoof their -- where they're coming from, their ISP. They can spoof, you know, all sorts of things. Many people are using this to trade music, to trade books, to trade movies, as the -- as the bandwidth increases. And -- and without an ability for people to be identified, it's necessary, in my opinion, for the Internet to have a system whereby people stand up for themselves.

If they are themselves, they're not some weird, you know, 12-

letter nickname; that they are themselves, and this is not a violation of their privacy. It -- it's just them being themselves. It's just like, in real life, if you walk down the street, you are yourself. You can be identified, and that's the way I feel it has to be.

I -- I don't understand. I don't see how copyright can be enforced on the Internet unless people can be held accountable for what they do.

BERNSTEIN: Even then, though, I think it's so -- so massive and there's so much piracy going on -- even innocent piracy, even admiring piracy. I think a lot of people don't understand that there's -- that for people who write articles, for people who write science fiction stories, there's a lot of resale value in a literary work.

You can place something in a textbook. You can place something in an anthology. Things are used in educational settings. So once something gets out and it's in a place where everyone can find it, the value of that work disappears.

And -- and I don't know what the solution is to -- to get it stopped, but I think that a lot of the things that publishers and -- and these big companies are doing are encouraging the idea that this work does not have -- have value. And that the person who created it does not deserve to be paid for it. And I think that somehow reinforcing the idea that people who are creative...

(AUDIO GAP)

SHANNON: ... books stores, and she got news that it had been adopted as an adjunct textbook at a number of journalism schools, including Berkeley.

And a young -- she lives in California, this member -- and a young friend of hers, whom she'd known all of this young woman's life, came up to her in great excitement and told her that she was taking a class and my friend's book was an adjunct text in -- in the class.

So my friend said, "Oh, that's wonderful news. I'm so excited that you're going to be reading it. Oh, swing by and I'll autograph your copy."
And she -- and the young girl said, "Oh, well, I didn't have to buy it. I didn't actually buy it. I just went to Google Books and, you know, you can get 20 percent. So I got 20 percent and my roommate got another 20 percent and then I signed on on another screen name and I got another 20 percent," and she went on in that vein.

She got the -- the entire book and then she found this handy-dandy little program that stripped all of the little dings and clicks and odd -- page oddities so that it flowed. And bingo, she had a PDF of my friend's book, which she then gave to several of her friends. And my friend said to her, "Don't you realize that this is how I make my living? And that you've known me since you were a little girl. This is my income. I write these books. You're stealing from me."

And the young woman was outraged, just outraged. She just didn't understand at all. That is the biggest danger, I think, of Google Books and the book search feature on some of these, is that there are all of these programs that can just bypass all of the safeguards and download as much of the book as you want.
And if you think that isn't true, search a little bit on the Internet and you will find a myriad of programs from China and Malaysia particularly, that for $29.95 or even less, you can override the controls on these and just download the entire book.

SIMPSON: Stuart, you wanted to say something?

BERNSTEIN: Yes, well, it's -- I think also what Amazon has tried to do in terms of bringing down the price of books also tends to devalue them.

It's one of the places where publishers have tried to stand up to -- to what, in a sense, is just trying to gain market share by selling books at the lowest possible price.

And using these -- these search programs, the Google Book search, the Amazon search inside the book, is a way to bring you to that site. They don't care if you buy that book. You're going to end up buying something or, with Google, they're going to be able to improve their search by watching what you do, what you're searching. You know, the -- the -- to me it's a -- it's Google is trying to just get all of these words and all these combinations so that it's -- it's something that they can -- they can riff off of in improving their search.

SHANNON: Exactly; 15 million books now.

BERNSTEIN: And so you have -- you have a situation where people who are responsible for creating our -- creating our culture are becoming beholden to people who really only care about a bottom line of market share.

(AUDIO GAP)

CAPOBIANCO ... and it was in print for about five or six years. When the books no longer sold a whole lot of copies, the publisher put it out of print, and at that point my contract specified that I could revert those rights and I did. It took a while, but I eventually reverted the rights to those books and -- and in 2000 I sold the book again to Harper Collins.

And this just demonstrates that an out-of-print book is (inaudible) something. It gets back to the author's control. It's not a dead book in any sense, and -- and people are saying that these out-of-print books, no one would be interested in them; that -- that they are completely worthless, but that's clearly not true.

And it's important to keep that distinction in mind. An out-of-print book is just something that has gone back to the author. The author is perfectly capable and -- and may very well be in a position to profit from it in the future. So when they take all of these out-of-print books away from authors, they are basically taking some of their future livelihood away from them.

I'd also go back and say that -- that the deal about the Google Book settlement is that it is opt out, as opposed to opt in. And maybe that's not clear to everybody.
"Opt out" means that you have to tell them not to do it or they will. And they -- if you do not, an author who either doesn't hear about this or their heirs may not know that they have control of this book because the copyright was inherited, they may -- that book can be used in any sorts of ways by Google down the road.

They may be able to sell an e-book. They may be able to do a print-on-demand book. There are only very small limitations on what Google -- Google can do with that book unless the author steps forward and says, "Hey, wait a minute, stop."

And this is turning copyright on its head. Copyright says it's an opt-in regime. The only time a publisher can publish your book is if you opt in. If you tell them, "Yes, I want you to do that." So that's -- that's why we oppose it.

SHANNON: There's also a little problem in that even if you opt out, when you read the fine print on what Google tells you about when an author agrees to opt in or opt out or when they were. They -- Google is not obligated to do what it says it's going to do now in future. It makes it very clear that in future if it scanned your book, even if you say, "No, I don't want you to have it, Google, I'm

opting out," they can change their minds. They make that very clear.

CAPOBIANCO: That's the capper from reading that -- i you read that whole long settlement, and it is very hard and impenetrable reading, at some point, about two-thirds of the way through, it says, "Oh, by the way, you know, we don't guarantee we won't continue to use your work even if you opt out."

SHANNON: Trust us.

CAPOBIANCO: Trust us.

SHANNON: Trust us.

CAPOBIANCO: You know, we'll -- we might do it, but trust us.

SIMPSON: Questions?

QUESTION: Yes.

SIMPSON: Could we wait for the microphone, please?

QUESTION: I'm -- I'm an author and a -- and a publisher as well. And isn't the Google Book settlement, isn't -- when the -- they're -- they're not just taking your book. Aren't we getting a payment back based on Google ads on the pages that go alongside of the books? Don't you set up a deal...

SHANNON: Well, theoretically.

QUESTION: ... to -- to get -- get money back?

SHANNON: Yes, theoretically, but do you remember how when everyone first began putting Google ads on their websites, we were all going to rich from the Google ads on our websites?

I suspect that it will be very much the same and the percentage of money for those hits and whatever is very small. It's a good -- it would be a very small return.

CAPOBIANCO: Well, there are a couple of ways that the Google Book settlement will supposedly pay people. One of them is if they scanned your book, part of the settlement is if they scanned your book during this period, prior to, you know, January of, I guess, last year, then you are due a $60 payment. If they didn't scan your book, they can still use it, but you don't get a payment.

Other than that, if somebody buys your book on the Google Books website, 65 percent goes to something called the book rights registry, which is an organization that is being created -- would be created by the settlement, primarily run by the Author's Guild and the AAP, the Association -- the American Association of Publishers; 65 percent goes to that, 35 percent goes to Google.

And if they -- if they do any advertisement on the -- on the web -- on the web search results, Google gets all of that. So 65 percent goes to this book rights registry. The book rights registry has the ability to deduct their expenses from it off the top, and that whatever is left would go, at least allegedly, to the author and the publisher.

SHANNON: And there -- and their own limits on the expenses; none whatever, nor is there any oversight whatever on -- on who is making sure that the rightful payments to writers go to the them. No oversight.

CAPOBIANCO: The only oversight comes from the book rights registry, which is, allegedly, you know, our negotiator or our representative in this process.

BERNSTEIN: And -- and just one other comment in terms of Google and -- and the web, in general, in terms of books. One of the books that I've done that I've pretty much turned over to the web, is a guide book. And my sales, the guide book was also a top selling, it's a ski guide in the country, but, you know, it only -- I might make $20,000 to $25,000 a year on it.

Once I turned it into a website, I put it up and I got it used. I mean, now my book is basically an expensive business card. And all of my income, my income's more than doubled from what's coming through, you know, from web advertising and from selling individual chapters one at a time and finding new ways to market them. You know, package those with coupons for ski areas and stuff like this.

And -- and so it's allowed me to take what -- where it was kind of locked in with, you know, with a publisher because I'd get a certain amount. All of a sudden now, you know, it opened up a whole new world, so I mean, there's -- it cuts two ways. And I understand the book (inaudible)...

CAPOBIANCA: There's -- there's no question that nonfiction, especially nonfiction like what you're talking about has a greater

potential to find an audience than fiction, for example.

Now, one of the things that -- that I've been wondering about for a while is how, OK, say you've every science fiction book ever written on a website. And the only mechanism for finding what you want is a keyword search. It's useless. You could look up "rocket ship." You could look up, you know, there's no way that a keyword search would help.

Whereas, your book, there are various keyword searches that would bring people right to it. And they'd get exactly what they wanted.

So there is a disparity there in -- in whether, you know, something can be profitable in the way you're talking about, or whether it's, you know, will just be lost in the -- in the -- in the noise.

SHANNON: I also want to point out that you own the rights to that book, and if you had a book that was caught up in the Google -- the Google Book search, and because the publisher saw that down the road there might be a chance to make some money off the book, even though it was not selling well and no longer in print, the publisher in all likelihood would refuse to give you the rights to the book back, which has been traditional.

And as Stuart can say, in the book business, rights have -- have, after a time, usually revert to the author. That isn't happening anymore because publishers see that down the road they might be able to make a nickel off of this. And I don't know -- I haven't heard of any member of our organization in the last year or two that has had rights to a book revert. It's just not happening anymore.

SIMPSON: (inaudible), I think you had a question.

(CROSSTALK)

BERNSTEIN (?): Well, I just wanted to applaud you because one of the solutions to this problem is to do it yourself, and rather than giving away chapters, you're selling chapters. You're figuring out a way like the iTunes model where they're selling individual songs. You're figuring out a way to do that and to communicate directly with the consumers and you're cutting out these people.

I mean, in a sense, you're using Google because it's -- it's probably the main way that people come -- come to find you. But I just have to applaud doing it yourself. And -- and rather than having

to fight about getting the rights back to a book, don't -- maybe -- maybe it's -- it's not going to be a good idea to give them to a publisher in the first place.

SHANNON: But if your book -- the point I want to make is if your book was caught up in the Google Book search and you didn't own the rights, the publisher still had certain rights. The publisher could do that and take all of the money.

(CROSSTALK)

SIMPSON: Gary Reback, please.

REBACK: Gary Reback. This time I'm wearing my Open Book Alliance hat. I was going to address a question to Stuart, but anybody can comment on it.

It -- it seems to me from my perspective, you've got to give us more help here in the sense that we kind of looked at the Internet and thought, this was going to be a great opportunity for -- for authors and creative people because it was going to free you from the shackles of a few big publishers. And you even made comments to that effect, as I recall, at the -- the Google Book settlement.

And of course, there are now enormous problems, but we've got to have a mechanism to get past this. You've got to put -- you've got to get to us a model...

(AUDIO GAP)

REBACK: ... people who are sympathetic because, otherwise...

(AUDIO GAP)

REBACK: ... pointed them out, we need a pathway to get compensation to authors. And I understand it has to start with education, but we -- we've got to find a vehicle to fix this problem because we really can't go advocate, you know, shutting down the Internet. We've got to make it work in some way.

SHANNON: There already is a registry, Gary. We already have a registry whereby authors are compensated when things are -- are published. The Google Book -- that was one of the points, you know, we made when we were writing those position papers and so forth against the Google Book settlement is that we didn't need to create a second registry. We needed to beef up the one we have and to make

people aware of their rights.

REBACK: This is something I didn't know until you pointed it out to me, but there is already a vehicle by which authors can be compensated...

SHANNON: Yes.

REBACK: ... in this way.

SHANNON: Yes.

REBACK: I -- I was working in the OBA (ph). I didn't know that it existed until you told me about it when I was on the verge of filing a brief without knowing that. I don't think most of the world knows that to tell you the truth. And that's a start at a vehicle for -- for solving the problem.

CAPOBIANCA (?): It is. And our organization, the Author's Registry, was created in the mid-90's and our -- our organization immediately signed up as many of our members as we could because we recognized that this registry was a way for people to find contact information for our authors if they wanted to buy their work. And unfortunately, it -- it hasn't moved into the 21st century.

I mean, authors, many of our authors who signed up in 1997 still have the same contact information because there hasn't been any updating process. And there's no way, for example, for an author to go online and update their contact information, which you would think there would be -- would be very simple.

SHANNON: But it could be -- I mean, if you threw a little money at it.

CAPOBIANCO (?): It could be.

SHANNON: It could -- it could be beefed up very easily if the mechanism is already in place.

CAPOBIANCO: The -- the ironic thing, to answer your question from my perspective, is that our organizations, CEFLA (ph) and ASGA (ph), all of the writer's organizations basically are prohibited from advocating or -- or negotiating for their members because of antitrust laws.

So we're kind of stuck. We can't -- we can't say, "Go out and --

and -- and negotiate a best practices contract for all -- all of our members" because it's against the law.

It -- it's ironic because the Author's Guild did not feel that that was a -- that didn't stop them from doing this enormous, you know, well, doing it through a class action lawsuit...

(AUDIO GAP

CAPOBIANCO (?): ... somehow gets around this, but, it's still, it's, you know, (inaudible).

(AUDIO GAP)

BERNSTEIN (?): ... where you're not -- you may be beholden to a certain platform that -- that you sell that app, but that then becomes a way for you to communicate with your readers and to control the -- the way -- the way material itself is protected.

So it's -- to me, it's a very vexing question because I feel like I've got my finger in a dike and it's -- it's, you know, you've got something like WikiLeaks, where all of this material can just be taken and -- and, as far as text, once it's -- once it's freed from (inaudible), it's just like going into a bookstore and browsing.

But it's not like going into a bookstore and browsing. You don't have to get up off your, excuse me, ass and go to a bookstore and you just -- you -- you do see people sitting and reading in bookstores. But it's -- it's very different when you have that instant access at your desk.

I had this argument -- I've been having this argument for years with -- with publishers about allowing people to look inside these books and have almost free access to them, in a way.
And I remember the first time I -- I wanted to -- to make some veal stew and I have all of these cookbooks from my years as a -- as a bookseller, and I remember pivoting towards the computer and going and finding on Amazon look inside Martha Stewart's recipe for veal stew, which I then took a picture of and printed it out. You know, forgive me, and I -- I sent it to Random House and I said, "Does Martha know about this?" I said, "I might have 49 cents for it or 99 cents for it."

So it -- it -- it needed to start early and no one was there watching how this happened. And I think it's in all -- it's -- as far as the news media, it's -- it's very similar -- wow to -- how to rein

it back...

(AUDIO GAP)

CAPOBIANCA (?): ... the right to do a search inside function like that, and the publishers have gone ahead and let Amazon do it without -- without having the -- the license to do that.

So it's really -- it's a double whammy. You're being -- you -- on both sides.

SHANNON: We also -- we also need to have, I think, a conference on practical solutions for copyright in the digital age. Our organizations have been talking that, and obviously involving the high-faluting copyright lawyers, but we also need people who will come up with practical solutions on how you can maybe have an informal -- a pay wall where you can pay 49 cents for that recipe -- ways to do it.

We know that traditionally, Congress doesn't act to revise copyright law unless it's under great pressure either from a corporation or a great outcry from the citizenry. And I think the great outcry from the citizenry is what we need, too.

SIMPSON: I -- I think we're starting to hear it.

SHANNON: We're getting -- we're beginning to hear it.

SIMPSON: I'm -- I'm going to have to very reluctantly bring this to a close, and thank the panel very, very much and -- and the questions.

What we're going to do now...

(APPLAUSE)

... is -- and we've been talking about the privacy report that came out today and in fact we're going to have some of the panelists who were earlier are going to be doing a response to that with a press call call-in right here, which we had not anticipated. And we're -- we're setting up for that now.

The chairman gave his briefing on the new report at one o'clock and this group has been through it. And we're expecting here very quickly to -- to get the calls coming in and doing that sort of press conference. And we'll want to be doing that web casting.

So thank you again very much.

END