FTC Informational Injury Workshop
December 12, 2017
Segment 4: Panel 3
Transcript

CORA HAN: All right. If folks could take their seats, we'll get started with this afternoon. OK everyone welcome back. Dan and I will be moderating this next panel, which will build on this morning's discussion, and explore how businesses and consumers perceive and evaluate the benefits, costs, and risks of collecting and sharing information in light of potential injury. The panel will examine the considerations businesses take into account when choosing privacy and data security practices. And also how consumers make decisions about sharing their information.

So we are lucky to have a great group of panelists here with us for this discussion, and we will take questions at the end. So just as a reminder, there are comment cards available in the hallway and also with FTC staff inside the auditorium. And if you just fill it out, raise your hand, someone will come and get it from you. For those of you viewing the webcast, you can submit questions via Twitter. Now I'd like to introduce our panelists.

So, closest to me is Omri Ben-Shahar, who is the Leo and Eileen Herzel Professor of Law and Kearney Director of the Coase-Sandor Institute for Law and Economics at the University of Chicago Law School. He teaches contracts, sales, trademark law, insurance law, consumer law, e-commerce, food law, law and economics, and game theory in the law, and writes primarily in the fields of contract law and consumer protection.

Next to Omri, is Leigh Freund. Leigh is the President and CEO of the Network Advertising Initiative where she leads the organization's growth and helps set the agenda and strategic priorities. Leigh joined NAI in 2015 after an 11 year career at AOL where she served as Vice President and Chief Counsel for global public policy.

Next, we have Jennifer Glasgow, who has served as a global privacy and policy executive for over 40 years. Originally with Axiom and most recently with First Orion Corp. She is very active in numerous international efforts to develop effective public policy with maximum harmonization across the world.

Then we have Bob Grourley. Bob is Co-founder and Partner of the cyber security consultancy, Cognitio, which helps companies fight cyber crime and corporate espionage. He is the author of the book, The Cyber Threat. His first career was as a Naval Intelligence Officer, and he was the first Director of Intelligence at the Department of Defense's cyber defense organization.

And last but not least, we have Katie McInnis. Katie is a Policy Counsel in Consumers Union Washington D.C. Office. Her work focuses on technology and the consumer's right to privacy, security, control, and transparency. Before joining Consumers Union in 2016, Katie served as a privacy and technology fellow at the Center for Democracy and Technology and in the Enforcement Bureau of the Federal Communications Commission. So thank you again to our panelists for joining us today.

DANIEL WOOD: OK. So the format of this panel is basically going to be a loosely organized group discussion. And we're going to start off with some business oriented questions. And the first one is pretty broad. So what are the risks and benefits businesses consider when deciding whether and how to collect and share consumer information?

LEIGH FREUND: You want to start?

JENNIFER GLASGOW: Go ahead.

LEIGH FREUND: OK. Good afternoon, everybody. Thanks for having us on the panel this afternoon. We're thrilled to be here. I represent the digital advertising industry here. And we represent third parties, first parties, and other companies involved in the digital advertising ecosystem. So when we think about the benefits and the risks and how companies are weighing the benefits and risk of the use of data that's collected online, we think through of the entire internet ecosphere. So revenues from online advertising support the free internet. I know that's a very broad statement. But we support and facilitate e-commerce, we subsidize the cost of content and services that consumers really value and expect. And this is a really, really valuable kind of benefit. We have to weigh that with the risk of what are we doing with consumer data and what our consumer expectations, which is something I think we'll get into in a little bit.

We've got some statistics to share with you. 85% of consumers in a survey that was conducted by the DAA-- which is one of our fellow trade associations-- say that they prefer an ad supporting internet model so that they don't have to worry about paying for costs and services. And so online marketing has really big, direct, significant benefits for consumers. It helps them connect, create, publish. We're talking not just about Google and Facebook when we talk about the internet, but we're talking about my favorite hypothetical example which is joesknitting.com. We can support advertising that supports joesknitting.com to be able to reach their consumers because the advertisements are reaching individual users as they travel across the internet and not individual web sites. And so we support kind of the long tail of publishing online, and content and services that consumers might not otherwise be able to access.

So when we think about risks however, part of our genre is self-regulation in this internet advertising ecosystem. And so we think about what are the specific concrete injuries that are likely to cause substantial injury or harm to consumers. We think through the Section 5 framework about how things are not reasonably avoided by consumers. And what are the benefits to consumers. And so we think through data practices that are reasonable. We try to think about the types of injuries that might be quantifiable and economically harm a person. We think through some things like eligibility for employment. We think about eligibility for insurance requirements. And now we collect and use a lot of data in advertising. And the serving of a targeted ad to you or to me because of our interests online is different, and so weighed differently than the actual use of that data to make a decision around eligibility for employment or other things. And so we've got guardrails set up in our own environment and our self-regulatory code that kind of thinks through these potential concrete injuries and puts restrictions on our company's use of that data. So when we think about benefits and risks we really try to spend some time thinking specifically about how to avoid the risks that might be inherent. We heard about some of them already earlier in the earlier panels. And try to put guardrails around

them so that we can have responsible, but vibrant, data collection and use throughout the internet.

DANIEL WOOD: Great. So actually to make things easier let's raise our name cards if you want to say stuff. But Jennifer, please go ahead if you're going to. Sorry.

JENNIFER GLASGOW: You want me to answer the same question, right?

DANIEL WOOD: Sure, yes.

JENNIFER GLASGOW: Well, my experience is in both marketing-- so I'm very familiar with what Leigh and NAI have done-- but also in risk management and government use of data. So I feel like when businesses are trying to assess the risks of information collected and sharing, they tend to start by saying what are the benefits? What are the opportunities that information creates? And the reality is-- and you probably got a sense of this from the morning panels for those of you that were here-- the reality is that every piece of information you collect has the potential for some benefit. And it may be different. It may be many, many benefits. Very rarely does a piece of data stand alone and only create value in one instance. However, there's two sides to that, or that sword is sharpened on both edges, because there are risks as Leigh has mentioned that need to be taken into consideration.

We look at laws first to decide is whatever activity we're doing compliant. Sometimes that's an easy call, sometimes it's a hard call. Because many of the laws I'm most recently working in the telecommunication industry. And we have laws going back to 1934. So none of those laws even contemplated the environments we're living in today. You have to kind of read between the lines and figure out what you should be doing, and what you shouldn't. Or what the intent of the law was. And then we have a lot of different self-regulatory groups, like the NAI and others that focus on very specific, typically either activities like marketing or industry sectors.

And I think it's a good balance because the industry groups can move quickly when new issues surface, or when new technology, or new business practices evolve. And if necessary you can back them up with a law on something that's really egregious or that industry is not able to get wide adoption for. So the risks? Most businesses today I think-- certainly those that have in any kind of international presence, with maybe the exception of some small ones-- go through privacy impact assessments on what their business is involved in. Any assessment you read, any of the standard guidelines for a PIA say you have to look at the risks. And you have to mitigate those to the degree that it's possible or to the degree that makes it acceptable. An acceptable level of risk versus the benefit.

DANIEL WOOD: Great. Katie.

KATIE MCINNIS: We know that businesses evaluate risks and benefits to data collection, but we also know that they exhibit the normal human tendency to overestimate the benefits of data collection in comparison to the risks. And we've seen this thanks to many data breaches recently. The companies aren't sufficiently internalizing the risks of all this data collection when they evaluate the benefits of such collection.

DANIEL WOOD: Great. Bob, do you have, as a cyber security expert do you have a--

BOB GOURLEY: Well, I would say that answers to questions like this I think vary from industry sector to industry sector depending on where you're at. For example, in the financial sector those companies are all built around trust especially if their consumer facing. So they take an approach where absolutely everything is evaluated from risk. Compliance is critically important to them. Any a heavily regulated industry compliance is extremely important.

We all know compliance does not equal security. And compliance does not automatically reduce all risk of data loss, but compliance is extremely important. Because if you fail it can be a company crushing event. So I would say my approach to questions like this is to look industry by industry. There are other industries where you're collecting information that is already publicly available. You're just pulling together and using it slightly different. So if that information is lost, is that any risk? Does it hurt your brand at all? was all publicly available. And so the kind of question like this I think it's very important to figure out what's the business model in the particular industry, what are best practices for that industry, and then what's the right approach?

DANIEL WOOD: OK. So is reputational injury important in advertising and privacy considerations as well?

LEIGH FREUND: Oh absolutely. That's why we're here. I think what we represent is people like Jennifer's former company and others who came together recognizing that with all of this data comes great power and great responsibility, to use a Superman analogy. But I think that thinking through-- it wasn't Superman--

BOB GOURLEY: Spider-man

LEIGH FREUND: Spider-man. Sorry Yes. I'm sorry. I have my superhero's wrong. You can tell my kids are out of the house already. So I think that we've got a group of companies that are dedicated to responsible data collection and use practices because there's a need for that. Consumers have said that there is a need for that. Industry and regulators have recognized that there's a need for that. There's been some talk of legislation with no actual legislation enacted here in the United States at least. But we think about Europe and the data protection legislation enacted there.

And so, yeah, I think especially in advertising. When you've got relationships with consumers by first parties but also the very backbone of that advertising community is made up of companies that are unknown to consumers. So it carries a bigger responsibility. So because you're not necessarily known to a consumer and you're collecting and using their information you've got to put certain safeguards in place. We have lots of safeguards in place through our self-regulatory code, some of them I mentioned. As the data gets more sensitive the restrictions get more onerous.

We have, for example, a definition of sensitive data within our code, and that covers a lot of some of the things that were discussed in the earlier panel with respect to health data. Some of those as the sensitivity increases the requirements for what you may and may not do with that

data, and the types of consumer notice and choice that you have put around that, is really important.

And so we base our code on the very basic principles of privacy, on the FIPS. And it centers around notice choice, accountability, and control. And so in advertising we think this is really important. I think when it comes to, like I said, the use of data to serve me a Nordstrom shoe ad just hypothetically is less injurious to me than the concept of somebody using something around HIV status, or gender identity. And so we've put guardrails around those things in our code to try to make sure that folks understand that they can trust. I think trust in advertising-- and I know a lot of what you folks have mentioned on earlier panels-- is the complexity of this environment. The data environment.

I'll use an analogy that is not my own but I'll use it anyway in terms of developing trust. So you fly on airplanes every day. But you don't necessarily know every word of what those mechanical manuals say about how that airplane flies. You just have to trust that the people that do know what they're doing with it. And so part of our purpose and mission is to help that consumers will understand that people know this very complex digital advertising ecosystem and the data that's around it will do responsible things with it. And by adhering to our code and the code of the DAA and other self-regulatory orgs out there, we think that we are striking that right balance between innovation and protection.

DANIEL WOOD: OK. So do businesses do-- I guess you've addressed this Leigh-- other panelists in your experience do businesses consider directly the injury to consumers?

JENNIFER GLASGOW: I'm sorry. Consider what? There's an echo.

DANIEL WOOD: Sorry. Do businesses directly consider the risk of injury to consumers?

JENNIFER GLASGOW: I think they do but I think it's really difficult for them to understand what those risks might be. Certainly the ones that I've been involved in, whether it's Axiom where I was employed or whether it was clients that we were serving, would ask the question, what are the risks? And I think from this morning's panel if I had said either I as a Privacy Officer for the company, or the company themselves, probably would have not recognized over half of the risks that were actually-- or the consequences that were actually-- discussed this morning. So I think there's an opportunity to continue to educate the business community about how serious some of these risks really are. Because most of them at least-- and I'll totally agree with Bob that it does vary from sector to sector-- and how regulated, or what kind of compliance obligations fall on the company.

But it is one of those situations where we need to understand all of the potential risks. And they're evolving. We have new risks that surface with new technology. And maybe the FTC in conjunction with industry could do some more with that. IAPP, the International Association of Privacy Professionals would be a great audience to carry those messages to the businesses.

DANIEL WOOD: OK. Katie?

KATIE MCINNIS: I just want to jump off of what Leigh was talking about with the differences between different kinds of information and the kind of sensitivity we ascribe to them. I think that what's getting complicated in the space is that with increased data collection non-personal identifying information is now quickly becoming personally identifiable information. So although you may not know my gender identity, you may know what kind of products I'm looking for online and therefore can make an inference that I have this gender identity. Or maybe you don't know my HIV status, but you do know that maybe I would be in the market for an at home test. So it does get very concerning this huge collection of data and the kind of inferences you can draw from it. And I think we need to be aware of the kind of data that you're collecting can really be highly sensitive even if the individual data points don't seem sensitive on their face.

DANIEL WOOD: And do you think businesses are inadequately aware?

KATIE MCINNIS: I think it's hard to tell. I'm not a business, I haven't worked for business. So that's a little hard for me to tell personally. But I do know that with the number of data breaches that have occurred, especially in industries that do not have a direct relationship with consumers. Equifax is a great example. We knew that there's a huge amount of data about individuals that they never really opted in or gave permission to be collected about them, but can have a really injurious effect on their livelihood. And also some clear informational injury beyond just financial injury.

DANIEL WOOD: OK, great.

LEIGH FREUND: Just quickly respond.

DANIEL WOOD: Sure.

[INTERPOSING VOICES]

DANIEL WOOD: Jennifer.

JENNIFER GLASGOW: I want to make a point that I think we need to think about data breaches in one light, and then we need to think about inappropriate use of information by the company in another light. Because both of them can be harmful. And quite often we conflate the two. And I think resolution and mitigation for those kinds of bad practices may differ dramatically between the two categories.

LEIGH FREUND: Yeah. So Jennifer took my answer.

JENNIFER GLASGOW: Sorry about that.

LEIGH FREUND: But I will add to that, that I think the concept that Katie rightly brings up is, what data do you need to do the action that you are doing? The less data you have obviously the less risk of data breach. And I agree that we need to keep them kind of separate and distinct. But in our case advertising data is only valuable in very limited circumstances and for very limited time periods. So one of the things we counsel our companies, our members to do, is practice very

good data minimisation. So if you don't need the data, and you don't need it any longer because the person's bought the car-- or in my case bought the shoes-- get rid of it. That is something that I think good data responsibility and good data collection practices and use will engender that concept of data minimisation. I think it's important.

DANIEL WOOD: Do businesses in general seem like they are cognizant of data minimisation and how important it is?

JENNIFER GLASGOW: I think they're aware of it. Again, it's going to vary with the industry and it may also vary with the size of the company. It's something that they talk about if there's any kind of international footprint because those are more regulated kinds of activities. In other geographies it becomes more important because they know it's important in Europe. And it's easier to just deal with it worldwide than it is to do things differently in one country from another.

But I want to caution against data minimisation being too much of a panacea. Knowing how long you need the data and how long it's useful is important. But some data has a lifetime of value. And so the idea that all data has an expiration date that's fairly short, may lead you into a situation where you're not maximizing the benefit you could bring to it. For instance, if you want to contrast marketing, which as Leigh says has a much shorter lifetime of value, to identity theft. If I have a pattern of where you've lived for the last 20 years, I can do a better job of predicting that you are the person you claim to be and than if I have two years of that data. It can be very variable.

BOB GOURLEY: I'd like to push on that just a little bit too and say, I have not seen a correlation between how much data you have and the likelihood that it will be breached. Your data needs to be secure even if it's a very small pile of data. And a lot of times a small pile of data and a small company is actually of greater likelihood of breach because that small company can't protect it as well. I would say what would GAFA do? We've got to watch what GAFA is doing because they're leading us all forward. Who is GAFA? What's GAFA? GAFA is the big industry players when it comes to data. Google, Apple, Facebook, and Amazon. GAFA is leading us all into how we're going to do privacy in the future.

And they're moving a lot faster than I believe the government, or even consortiums can. And they're adopting things like very smart encryption. Ways to stripe and secure data and spread it around places where it's harder to penetrate. Not perfect, but harder. They're also advancing cryptologic concepts called, differential privacy. Have you guys heard of differential privacy? It's a cryptographic construct that has been around for several years. It was now brought into Apple's iOS 10. So we're all using differential privacy now. We didn't even know it. It's in Apple. Facebook is using it, Google is using it.

And what it does is allows you to extract data from data sets in ways that do not really reveal the underlying data, but give you statistically meaningful information. A simple way to think of it is when you use the traffic on your Google Maps and it says that it's red on this road. It knows that because they're watching the traffic. And they do that in a way that does not take away the privacy of the individuals and how slow they're moving. So my bottom line point to all this,

watch GAFA. Watch where the big guys are going with privacy and protecting data. I think it's extremely important. So the question to ask yourself, what would GAFA do?

DANIEL WOOD: OK. So we've heard the various factors businesses take into account in thinking about the risks and benefits. So maybe GAFA. The trust that the consumers are placing in them, the consumer expectations, compliance, and regulatory issues, and the concrete injuries possible to consumers. How well do these factors businesses consider correlated with potential injury to consumers? So how well do the various factors businesses think about when they're weighing whether and how much data to collect and share correlate with the potential injury to consumers?

JENNIFER GLASGOW: I'll start it off. I think this is where I want to answer the question first from a security breach perspective and then from an appropriate use of data perspective. From a security perspective, I think they correlate pretty well. We're now looking at all kinds of security related to data at rest, data in transit, and so on. And to pick up on the GAFA analogy, the fact that we're using cloud computing-- where many of the security precautions that a small company would never be able to put in place, or made available-- is actually a really positive step forward on the security side of the house.

Now that doesn't help at all with internal use of information and whether it's appropriate. And I think that we're beginning to realize that as data becomes part of every business practice regardless of what it is-- and much of it is personal data-- whether it's anatomised or not, it has both opportunities and risks. And those need to be evaluated as carefully as possible.

I used to say that we could put some guidelines out there whether they were self-regulation, or legal guidelines, that gave companies guidance about what they should and shouldn't be doing. But as information has proliferated everything we do, and the opportunity, the analytics that we have, to turn it into valuable insights gets very easy to do. Not just available to large companies with sophisticated data scientists. We have surfaced a different issue and it is every single use of data in a company needs to be looked at through the lens of a privacy impact assessment. And that should include the risk to the individual as best they can assess them.

If you look at an industry such as the risk side of the house where you're doing identity verification to try to understand if you're dealing with legitimate people. Or may have been required by law as it does with Gramm Leach Bliley, where there's a know your customer rule to actually verify that you're dealing with who you think you are. Those are industries that really pay a lot of attention to these kind of issues. I find that some of the tech industries, and some of the startup industries are not as consistent, if you will, in their evaluations of the internal uses of data outside of security.

DANIEL WOOD: Katie?

KATIE MCINNIS: Data security should be in line with what a consumer expects and what the business is really putting a high priority on. However, the number of data breaches we've seen, even just in the past five years, show that that isn't insufficiently guarded. We have Aetna, Uber, Yahoo, Equifax. So many companies have not sufficiently protected the data they were entrusted

with from consumers. And that's highly concerning and that should be their priority. And that's what consumers expect. And yet we're not seeing that being fulfilled.

And as far as misuse of data or privacy of consumer data, we're also seeing that that's not necessarily a priority. One good example is Uber's recent breach, right? They had a breach, they worked to cover it up, and then they also misused some internal data in ways that consumers felt was really, really creepy. And it led to some changes in their policies. And we see that change in their policies because they are consumer facing and they depend on this consumer trust. So yes both of these things should be important to companies, especially data security, but we're not seeing sufficient protection of either.

DANIEL WOOD: OK. Leigh?

LEIGH FREUND: Just a couple of quick things. One is when we think about our industry in general, I think it's important to keep in mind that without the consumer clicking on an ad none of this is here and none of this works. So obviously keeping the consumer kind of top of mind as we go through these processes is important. Whether or not we do enough is a matter for debate. But I do think it's important to think about-- Jennifer mentioned it's harder for some of the smaller companies, the start-ups and the smaller tech companies-- to put privacy top of mind due to either resource constraints or other things.

And I'll say, just a little plug for us, that the compliance process that we undertake with our member companies, big or small, is the same process for every company, every year on an annualized basis. And that helps make them put a priority on privacy that wouldn't otherwise be there. And I think we have-- Anthony my compliance person, a VP is sitting right here-- and he can tell you the rigorous and onerous process that folks go through. But I think it's important when you think about consumers and putting them at the cornerstone of things the priority of privacy becomes really important. And so we build things around it that help us make sure that even the smaller tech companies and the start-ups put a priority on privacy.

DANIEL WOOD: OK. Great

CORA HAN: Great. Thanks. So, Leigh I want to build on something that you just said. Putting consumers sort of at the front of mind. And my question for you all is, do businesses think consumers are informed about the benefits and risks to consumers from collecting and using their personal information?

LEIGH FREUND: Yeah. I think that is something that folks will probably disagree with on, even among our panelists here. But I think one of the things that we do, at least for our industry, is make sure that our members are aware that one of the cornerstones and pillars of our self-regulatory program is consumer outreach and education. That's part of what they're required to do as part of our compliance process, et cetera. So we try to make through either our own organizations efforts or through our member companies, try to make consumers aware of the fact that they do have choices about what happens with their data, and try to bring folks to our website where they can learn more about what digital advertising is. What why am I being targeted? Why is this ad following me around? We have some educational components of our

website that try to help people understand that a little bit more and help understand what the options are if they choose to exercise them.

I think in general we have found through some research that consumers are becoming more aware. I think this is where self-regulation has an advantage over some of the other types of things that we could do like regulation, or legislation, because we can respond to things a little bit more flexibly and quickly as new technology is developed. . But I think consumers' expectations are also evolving in this area quite a bit. I think about what we know and understand in the industry, but also about my parents living in Michigan who didn't grow up with this technology. I think they're listening. Hi mom and dad. And what their expectation is might be completely different from the folks living in Silicon Valley, or the folks living here working in this industry. So it's really incumbent upon the companies to try to use those efforts to make sure that they're understanding, that they're trying to educate the consumers about what their choices are and what type of data they use. I mean privacy policies, we can argue that those aren't necessarily as informative as perhaps they should be because they're buried. But trying to think of proactive ways to make consumers informed is really important, at least to our companies.

CORA HAN: Thank you. Omri.

OMRI BEN-SHAHAR: I would like to take an issue with that. I'm deeply skeptical about education, transparency, privacy policies. It's a nice kind of things for the companies to brandish and for the law to require. But it has no effect whatsoever. We know that for a fact from numerous studies. And there is no way to make it work either in part because you have to realize we're sitting here talking about privacy. But there are panels around the country and around this city and around where everybody is talking about other aspects of the consumer transaction. That consumers care and some lawmakers and some advocates care not less than data privacy, for example. The choice of forum arbitration clauses or the ALI cares a lot about the warranty disclaimers, and the way laws are being completely disclaimed.

So it's hard to educate consumers about everything and especially about data policy because it's a moving target. It's advances so fast. By the time people catch up, they are already two or three years behind. That said that doesn't mean that consumers don't largely understand what's going on. I think maybe there is some indication that they do. I can't say that is a fact. But people say in surveys that they are concerned about what's going on. That means that they think that the data collection, and data usage, and sharing is done in ways that they can't pinpoint the details and they will not be able to understand. But it causes them concern. So I think that there is a sense of the risks that comes maybe from experience and from some other context, not from privacy policies.

The other thing that I want to say about that is that I think consumers view-- return to the basic point-- that consumers view data policy as one aspect of the transaction. The data collection, and practices of firms is, in part, consumers view it as a good thing. Privacy, or information, is the new money. Said that before. People are delighted to pay with information, rather than with money. I mean they probably would prefer to do neither. But I think that there is a general understanding as well that there is a grand bargain here where information becomes the currency.

Also personalized services are largely good. People enjoy them. There's both a great, private benefit. I mean this is a symposium about informational injury, but I think from a social point of view we really also want to think about informational benefits. Catherine Tucker, who sits here and we'll talk later did some work about the value of personalized surveys of digital medical records and the lifesaving effect that they have.

I've looked at some work that is basically digital records and data collection in the auto insurance industry, and these pay as you drive arrangements-- that are by the way, prohibited in places like California because of privacy concerns-- and that value that they can bring. Some say estimate it could be as much as 20% reduction in accidents. When the insurance company knows how you drive, and when you drive, and how much, and where and how abruptly you stop and things like this, and changes the premiums accordingly, that creates maybe a privacy issue. But it also leads people to drive in a safer way.

One estimate that I saw is a reduction of up to 20% in auto accidents. That's like 3,000 lives a year, I don't know, maybe more. There must be a very large privacy concern to override that benefit. And I'm not even talking about the fact that people who's pay as you drive habits are measured drive less. Another estimate is about 8% less. That's an enormous reduction equivalent to the $1 of carbon tax. So there is an environmental benefit. There's also a benefit here to low income drivers. They usually drive less so they will get lower premiums. All of that stuff comes as benefits that come from data collection that consumer, if they are enjoy them, are enrolling into. They like these things. That's the context of what the people realize.

Of course, there are the bad things that people are either not aware of or when these things that hurt them. And I can say that this is considered by consumers as worse than other quote unquote, "fine print things" like termination fees and cell phone contracts, or warranty disclaimers, or things like this. To wrap up, consumers are aware that this thing is going on. They are not aware of the details and how advanced some of the collections are. But not concerned enough to buy privacy shields that are not that expensive and to protect themselves from these things.

CORA HAN: Thank you. This is a great transition for us into sort of the consumer perspective, and how consumers weigh the risks and benefits in determining how to share their information. So Jennifer, and then Katie.

JENNIFER GLASGOW: I'd like to propose that consumers have things they expect to happen. And I think security certainly falls into that category. We don't give them a choice about security. That's a must do. Whether we do it well or not is something we can debate. But then there are things that we should give consumers choice about. Online advertising as Leigh's organization has put forth. But I tend to be a bit skeptical about their understanding. And I think we need to separate notices and policies from understanding.

I've been knocking around this information world-- and I started out on the technical side of the house many, many years ago-- and I find that even as a professional it's sometimes very tedious for me to understand what all is happening. And I think as we move into more big data applications, and more analytics, where decisions are being made by the analytics engine it's going to get even harder. So I feel like we're going to have to get industry to rally around setting

guidelines like the marketing digital advertising industry has. The industry has to follow and that we don't have to ask the consumer choice about. Because there's a lot of research that shows that when consumers are given a choice, if they aren't sure about what they're really being asked they take no action. So that means the default becomes extremely important in terms of, is this going to be something that's allowed, or is this going to be something that happens, and they have an opportunity to stop.

CORA HAN: Thanks. Katie.

KATIE MCINNIS: I do think that there is an understanding that consumers have. To a certain extent they are trading information for a free service. I think people do generally understand if they sign up for Facebook, they're trading a certain amount of information away in order to use this free social platform. However, I don't think that that's always the equation here, especially when you have a number of unknown data brokers and other companies online that are collecting my data at a rapid rate. I have no understanding that I'm getting anything from them by their collection of my data. And nor is there any benefit to me.

And I also want to challenge the assertion that people want personalized services. Yes, to some extent I would benefit from personalized services from some of the organizations and companies that I interact with. But on the whole I do not want targeted ads across my web service, which is why I am one of the many users of ad block services. And the increased use of ad block services is showing that people do not really want this supposed personalized service that we so think they want. The personalized service also is clearly not about me but about making revenue on the other side. I think consumers do understand that.

And as far as how much consumers are understanding the kind of disclosures they agree to, I agree it's incredibly hard and there is a lack of complete understanding, in part, because a lot of it's happening on the back end. Which is why you have even, Facebook, that does a lot of work to make sure that you know what kind of people are seeing your data. People are still asking if Facebook is listening to them. So there is this gap of understanding of, oh I allowed my contacts and therefore, that's why they're recommending a client that I saw last week on Facebook. So there's this gap in understanding, and I don't think we should really always put that on the onus of consumers, right? And that's one reason why other intermediaries, like Consumers Union, is here to try and help evaluate the kind of policies and disclosures that are out there and help consumers decide which companies and which products to use.

BOB GOURLEY: I have a comment.

CORA HAN: Leigh, then Bob.

LEIGH FREUND: Bob, please go ahead.

BOB GOURLEY: Well, first of all I like so many other people I love Consumers Union. I'm so glad that you guys are doing what you're doing because we all need that. And I also want to say that I feel ignorant after studying these things for decades. And I realize I don't have a full understanding of what it means with my data is breached and lost. Sometimes I get angry and I

know it's wrong, like the OPM breach stealing my data. That was bad. It was horrible. But it had no real cost to me. Or the Equifax data breach. I got angry like $190 million other people because the data is out there.

But as I thought about it, I realized that had zero impact on me. I locked down all my credit records anyway. It had a big impact on that company because they're in the business of selling my data, but that's not my business. It didn't hurt me at all. My data had already been stolen. And my social security number is out there. Why? Because I was in the Navy. And every year that I got promoted it was in the congressional record. Here's Bob Gourley, this social security number, achieved this rank. So with that data being stolen, it has zero impact on me. So how am I supposed to quantify that? And for me, I don't want any of my data stolen, but I have no way of understanding if there's a big breach what the cost to me is. I do want my privacy protected like everybody else. What I do is my business. But I'm not quite sure how to quantify, or put a number, on the impact of a breach.

CORA HAN: Leigh.

LEIGH FREUND: I just wanted to touch quickly on the ad blocking issue. Folks that don't want targeted advertising, many of them download ad blockers which actually block the advertisements that are on your site in general. I would say the answer to that is go to the NAI website and exercise your opt-out. But I will say that we've done a lot of work through some coalition building in our industry on the concept of ad blocking, and we're realizing that privacy is not the top reason that people are downloading ad blockers. It's not that they don't want targeted ads, it's that they don't want their data to be used. It's that they don't want a terrible user experience.

And I'll suggest that when we use targeted or behavioral advertising and try to use data minimisation to not use as much data as we need to do that it actually creates a better online experience for users to get the same economic value out of a targeted ad. When you're not using data, you'd have to have 20 popovers, 20 pop-unders and some flashy, jiggly belly ads on the page in order to try to make up that revenue for the publisher. So ad blocking is harmful to that kind of continuation of the free content and services on the internet. And the reason people are using it is not necessarily privacy related, although it is one of the reasons it's kind of down the list.

CORA HAN: Katie.

KATIE MCINNIS: I just wanted to touch on something that Bob highlighted, which is these injuries to consumers are highly contextual, right? You have an instance in which OPM, an organization you knew about had your information, was breached. And you already knew about this and therefore acted proactively and froze your credit reports with the three major credit bureaus, which is great. However, for a lot of people first of all, they didn't have a relationship with Equifax. So they were surprised not only that their data was breached, but also weren't really sure how to handle it. And secondly, now they had to go take the step you did a while ago, and therefore they don't know what kind of future injuries could happen to them. In addition to the fact that a lot of this information is immutable, like a birthday, et cetera. And so the injury

maybe it hasn't happened now and it's hard to quantify but it could happen in the future. Which is one reason why it's so hard, especially for regulators and other organizations, to really analyze and understand what kind of injuries these cause to consumers because it is so highly contextual.

CORA HAN: Omri.

OMRI BEN-SHAHAR: I'd like to touch on some of these issues that Katie raised. I think that the question to all of us, what I said and others, what do people care about? I think that that's the key issue. Not what do people say they care about, but what do they actually know when there is stakes on the line, care about. I don't think the FTC should listen to privacy advocates, or privacy skeptics, to alarmist or deniers in either side about saying, hey I download ad blocker. People We are not representative of anything.

Also, I don't think that the FTC should listen very much to what people say in surveys they care about because they'll say they care about anything. There's a lot of things just don't add up. The question is what do their behavior shows when there are stakes, real stakes, on the line. When they have to make hard choices. What to spend the money on. Or what to sacrifice. Or what burden to take. What kind of popping ads and all sorts of these things flashing, non-personalized ads, to suffer through. So as to not be personalized then maybe they'll say, you know what maybe I don't care about it that much. I think these are the questions that determine whether there is an injury, in a sense, that is meaningful. Otherwise, it's all arm waving about either biased people that do not represent anyone, or people say things because the context they were asked. They say, oh yeah. Since you asked about data sharing, sure I care about it. What does that mean?

CORA HAN: OK. So I wanted to build on both Omri and Katie's comments. Oh actually, Katie, did you want to?

KATIE MCINNIS: Yeah, I just wanted to quickly respond to Omar.

CORA HAN: Sure.

KATIE MCINNIS: If it's OK. I take your point that survey data isn't indicative of what consumers are actually going to do. I hear your logic behind that, and I just want to counter that maybe there's something else going on here. Maybe consumers just don't feel like they have the tools to effectively make sure that their preferences are appreciated across many devices and services they use. Which is one of the reasons why the FTC launched their IoT contest last year was to try and come up with a way that consumers can control the different devices, and services they use within their home. To make sure that preferences are respected across platform and device.

I think the consumers feel like they don't have a lot of tools. Which is, to be fair the industry is hugely fragmented, these policies are really, really long and hard to compare. And even when you're in the market for privacy protective service, like a virtual private network, is sometimes hard to know what kind of services you're actually receiving. CDT's recent work and complaint to the FTC highlights that even if you're presented with these statements of what it's going to be

protected you're really unsure if that's actually going to be follow through on the back end. And that's one reason why these policies and privacy statements are so important is because, in some ways, that's the only way we know what companies are doing with our data information and the only way to effectuate those choices.

CORA HAN: Thanks. I wanted to back up just a second because Omri and Katie both talked a little bit about context. I wanted to give the other panelists, and also them if they have additional thoughts, to weigh in about how the context, or kind of data being shared, matters when you're thinking about how consumers are making those decisions.

JENNIFER GLASGOW: You want me to start? I don't think other than just sharing sounds scary. I don't think most consumers really think about it because I don't think they understand it. Data sharing goes on in all kinds of ways in every industry. If I think about the doctor sharing data with a specialist they've sent me to, and they send your regular medical records over or whatever. Every industry has a different kind of sharing practice. It may be with a third party who you've outsourced work to, it may be with a delivery service that's going to deliver the product to the consumer. It goes on all the time. So there are some things that the consumer touches and feels, and understands That FedEx is going to see the package that I ordered from Amazon, or wherever. But when it comes to what goes on behind the scenes, I think they're pretty clueless.

LEIGH FREUND: If I could add onto that, I would just say I think that consumers probably have a different understanding. When we get consumer complaints to our sight we get, I got a targeted ad. Stop using my social security number. You So the concept of what kind of data people have-- I think the sharing is scary comment is really important-- because I think consumers feel like, for instance, if you get a targeted ad you must know my social security number, my address, my credit card, and my Nordstrom frequent shopper card. When really it's a binary decision made by usually an algorithm that says, do I serve this consumer this ad, or this ad? And when you're talking about the concept of injury on top of that, I think it's important to remember consumers-- and I think it's important to try to continue to educate consumers as much as we can-- but I think that's where the airplane analogy that I used earlier and the trust factor kind of factors in. If you're on a website, or are using a provider that you trust, or that you feel like you can exercise your own choices with respect to that, then you're going to have trust and you're not going to have to understand the complexity of the ecosystem to feel like your data is safe. And security, I know, weighs into that very heavily.

BOB GOURLEY: We can talk about that to, the security piece. Depending on what your business is there's already security architectures in place to exchange data securely with consumers, especially in the finance world. If you've done a mortgage recently, you have to get documents to your mortgage provider. There's secure ways to do that. In my business, we used to do a lot of work by email. There's been a big shift in business recently towards very secure channels. Signal, Telegram, Wickr are key providers of these secure capabilities where you make sure nobody can eavesdrop on your business chattering communication with other businesses.

I think that's going to grow significantly and begin to reach into consumers too. So the consumers won't have to share information by email, which is really vulnerable unless you're

using a big provider like GAFA. GAFA does secure email. I trust Google, Amazon, Facebook, Apple when it comes to email. But other than GAFA, if you're using any other provider, it's unsecure. And so you're sharing information with a company. That company is storing it in some server somewhere. And it could get breached, or lost, or some employee could hit a button and send it to someone else. There's a great room for new architectures, and new solutions, that will improve consumer privacy and protect business information through these secure solutions like Wickr.

CORA HAN: Thank you.

DANIEL WOOD: We've been on this topic for a little bit, but what other obstacles to consumers face in evaluating the benefits, costs, and risks of information sharing? Omri?

OMRI BEN-SHAHAR: Well, I think the main obstacle is complexity. Everything in the consumer world is complex not just data policy. You can make things really simple for consumers if you really wanted choice. Every app, every website could have a very clear button. Do not track, shut down all data collection, and everything. That would make things very simple on the face of it. But of course, it's not because many other elements of the transaction depend on the fact that these businesses can harvest information and provide, sometimes depend for functionality, other times for profitability and the cost of the service. And now if you shut down the data collection. If the consumer simply clicks that button other things pop up. Well, actually now you have to choose, do you want the premium version that gets your pay for things like this. There's no way around the complexity of this aspect, and then once you throw in that every one of those consumer transactions has other elements that other-- as I mentioned, other audiences not in this room today-- but other audiences think they are the most important ones. Democracy depends on them. Like class action waivers, arbitration clauses, and the like.

OMRI BEN-SHAHAR: How many buttons do you have to give consumers to click an unclick? And how often do they have to do it? Because every website and every app has to have this. So you see it's becoming an infinite task of choice, and I think any reasonable, emotionally sound, and rational consumer would say, please don't burden me with this world of autonomous choice.

DANIEL WOOD: Jennifer.

JENNIFER GLASGOW: Yeah. I just totally agree and I'd like to add two more factors to the one, what do they understand? What is that it is constantly changing. A company that didn't have good security practices may have decided they wanted to go use AWS and has now under very good security practices. So the fact that you make a decision at a point in time either do something or not something, you might want to re-evaluate that on a fairly frequent basis.

The other piece I'll put on the table, which I think is going to be more and more prevalent in the coming years, is the whole idea of big data and very analytically driven business models. Where it is the computer that's making the decision. And we obviously have seen a lot of that in the health area and it's got fabulous results. We see it in cities, we see it in advertising, we see it in everything we touch. But I think it's going to make it harder and harder for the consumer to understand how you went from point A to point B.

And I'll give an example of that that goes back many years. There has been a very, very high correlation between insurance claims and your credit worthiness. And across the states, many of the states, the legislators did not understand that correlation. Whether or not the industry did a good job of explaining it I can't say, but they didn't understand the correlation. So many, many states have passed laws that restrict the use of credit information relative to insurance claims. And so that is a valid statistical piece of information that would help-- it may not help an individual who has bad credit-- but it would certainly help those that do to differentiate good practices from bad practices. But we're barred from doing it today by law. So that's what you've got to be careful, the trap you don't step into.

DANIEL WOOD: Katie?

KATIE MCINNIS: So as far as consumer obstacles in this space, we've talked about the long policies and how it's difficult for consumers to evaluate those. We've also discussed the difference between a consumer facing organization and an organization that has no direct relationship with the consumer where there really isn't this array of opt in or opt outs even available to the user. And those are two huge obstacles to consumers. And another one is that they really do have a hard time prioritizing future risk of disclosing this information when they're facing an immediate problem setting up a new device, or a new service that they really want the service from.

I think part of that is also due to the relative immaturity of our market. IoT devices offer a huge amount of functionality to users and they definitely want to take advantage of that. But a lot of times they're not able to even assess the security or privacy concerns within those devices, or adequately assess the privacy policies as compared to another device. Which is one reason why Consumers Union, Consumer Reports launched our digital standard last March to begin evaluating products and services under privacy and data security, but also in connection to the kind of services that these products can provide to you. So I may be wanting a new TV and I'll be able to assess the kind of colors, and richness, and use of the TV, along with the security and privacy of these TVs, and compare that to other models. And that really does allow the consumer to effectuate some choice where we're taking into account not only the service of the product, but also the kind of data and privacy security concerns.

OMRI BEN-SHAHAR: I want to say this. Maybe I pose it to a question to Katie. But my impression is that there are services in the market when we heard Professor Acquisti, Alessandro Acquisti, from Carnegie Mellon. Carnegie Mellon, nonprofit effort to rate the privacy performance of mobile apps at privacygrade.org. Now you have this information all boiled down to a single score and yet I don't have the impression-- again maybe I'm wrong-- that consumers are swarming to privacygrade.org to get that. If these kinds of efforts are failing, what does this tell us about the underlying question that we are all sitting here today to discuss, which is what is the consumer's injury from the existence of these practices?

KATIE MCINNIS: I don't think that we're failing, I think that we're really just trying to catch up. Bob pointed out a lot of these tech companies are moving much faster-- and I think Leigh and Jennifer also mentioned this as well-- that tech companies are moving far and beyond faster than regulators and other kinds of checks and balances on this industry are. And that unfortunately is

just how it is so far, but we're trying really hard to catch up. And just evaluating the privacy and security of apps to me doesn't create a full picture, right? Even if I know that this might have bad privacy security I'm only using it for some limited use. So I might not really care. However, something that has more personal information or attracts my everyday life, like a calendar app or a fertility app, I would much more highly prize privacy and security in that case. And I do think that you have to present a holistic picture of these products and devices, which is what we're trying to do in the digital standard.

But you can tell how hard it is because not only do you have to effectively assess the privacy and security And for our part we can't assess what's happening on the back end. We can only look at the device itself. So even then we're not even presented with a full picture of what the company is doing with your data. So I don't think it's failing, I just think that we're trying to catch up. And it's extremely hard, especially with the number of devices and products that are in the market. So we hope that we'll be able to change the marketplace, watch the space, and we'll be talking about some of our results in the coming year. But just because it's hard for consumers and hard for intermediaries to do this kind of work doesn't mean that we don't have an interest in it.

DANIEL WOOD: OK, great. So let's step back a bit and ask maybe a related question. Is there a robust market for privacy products and services? Why or why not?

KATIE MCINNIS: If I could just jump in on that. Yesterday Citizen Lab out of the University of Toronto released a new security planner tool, which is a personalized experience for consumers to go through and answer questions based on not only their concerns with their online data, but also the kinds of products they use quite often. And then it presents them with a hierarchical list of what you can do to help protect yourself online. And also gives an assessment of how much time and money it's going to take for you to implement these different choices.

And that just released yesterday. We already have over 5,000 unique hits to the site. Which is showing that people really do want these tools, it's just really hard first of all, to effectuate these concerns of preferences across all of your devices, but also it's really hard to get a handle on your security online. And in some ways it's good to just highlight a few areas, which they are doing on their security planner tool. Also the number of individuals [INAUDIBLE] the survey results, as Omir pointed out, doesn't necessarily mean action, but people are very, very concerned and they've been pushing for better protections online. We saw the backlash after the Congress reversed the broadband privacy rule under the Congressional Review Act. People really care about their privacy, they just feel like they don't have the way to really effectuate these concerns effectively.

DANIEL WOOD: Bob did you have something to say?

BOB GOURLEY: I do, I have a couple of comments. One, I agree-- this is get really hot-- because all of us are buying all these devices with chips in it. Internet of things. The average home three years from now may have 600 devices in it that have chips that are communicating with your Wi-Fi, with Bluetooth, with each other by this ZigBee. And these things have vulnerabilities and we're going to need tools like this understand how to protect our homes. There are commercial products available now that are aiming at the consumer in the home. The

three biggest as far as I know are, Symantec has something called the Norton Core, Bitdefender has something you can put in your house, and then there's something provided by, let's see Norton, Bitdefender and Cujo, is another one.

And what these things do is look at all of your internet of things devices, and see what's normal. They report back. So you have to opt in to information sharing. You have to trust that company. You pay them a couple hundred dollars a year and they have a team of people watching your devices. How many people are going to pay for that? A couple hundred dollars a year. That remains to be seen.

I would also say that Jennifer reminded me of something, and that is the analytic tools that are out there now may very well be a key threat to privacy. Right now many of us have either the Android smart phones or the Apple smart phones. If you get a call sometimes it will say, this call is possibly Tina because of a email you received a year ago. It had that phone number in it. That's, in a way, creepy. That's not my contacts. They're going through my email and reading it through machine learning. Or you start up your car and you look at your phone and it says it will take you 44 minutes to get home from here. How does it know I was going home? Well because that's what I usually do that time of day.

Now these are all examples of very discreet, little, machine learning, artificial intelligence solutions. But this stuff is growing now like it's on rocket fuel. If you look at Pinterest and what they can do now. If you pin an image they now have machine learning tools that can look at that image and say, that's not just a brown handbag, but here's exactly the type. And you may be interested in the following shoes. And did you know that when you were putting the image up there? And just watch this space of artificial intelligence and machine learning over the next three years. It really is on rocket fuel. And there are going to be privacy and security concerns that none of us have thought about. And that also applies to your medical data. There's going to be analytical tools that look over all your medical data. And all of a sudden you get called in for a meeting with the doctor you weren't expecting. And maybe that's good, maybe it's not. So there's so many of these issues that we just haven't thought through yet.

DANIEL WOOD: Omri? I think Omri was first.

OMRI BEN-SHAHAR: Well, as Bob mentioned there are options that are sold in the market to enhance one's sense of privacy and data protection, maybe also for security. Not an expert on that but I have this strong sense that if there were demand there would be supply. I recall that when the previous FCC was enacting its privacy rules, and I looked at it and I noticed that companies like Comcast and AT&T are offering no data collection packages Premium packages. It's just $25 more per month. And yet, if I recall correctly, not many people were purchasing these options. Suggesting that one of two things can happen. Maybe people really want it but they don't understand. Or people don't want it. I don't think that we can just proceed by saying, no matter what the evidence is we'll say, oh people just don't understand. If they did, they would want it. I think we have to consider which of these two explanations is the right one. And that would have to be an empirical answer. Do they want it and don't understand. Or do they not want it.

And one other quick observation is. A study that was done, my colleagues looked at the privacy practices of different websites, and they found that websites that deal with more sensitive issues have heightened privacy practices. For example, adult sites don't share information. Cloud computing sites have security measures relative. It's all relative. The only explanation for this is that there is some response to what these sites perceived to be priorities of consumers. So I would call that some form of a market response.

DANIEL WOOD: Jennifer?

JENNIFER GLASGOW: Just real quick. I'd like to differentiate privacy products that are directed to the consumer versus privacy products that are directed to the business. I'm a little skeptical that we're going to ever see really widespread adoption of the consumer products for all the reasons that we've been talking about. But I think the business community is very hungry for privacy enhancing technologies and products that they can build into their products. Because it may be far more tedious to develop the same kind of encryption or other type of activities that you would want to make more automated. So I encourage the development of commercially oriented privacy products.

DANIEL WOOD: OK, great. So I think we're going to move on to audience questions. The first one, which is maybe to the business folks, but feel free to answer it. Anybody. Is how do the panelists define or quantify reputational harm?

JENNIFER GLASGOW: Well I'll jump in there. I think reputational harm is a harm that's evolving, and it's evolving in a pretty rapid rate. If you think about it, it varies whether we're talking about harm to an individual or harm to the business entity. Because reputational harm could come from both. We've had reputational harm in the business community from security breaches. Although, I'm sad to say-- and I don't have statistics to back this up, this is just my personal assessment-- that I think people are getting a little immune to security breaches because there are so many of them. And therefore, it is less of a differentiator from a company that has had one or hasn't. And I think that shows consumer has given up. They don't know what to do about it. They can't fix it. And even if they're, as Bob described, a victim, then they're not really sure whether there's anything to get panicked about or not. So I think that we've got a lot of work to do there.

DANIEL WOOD: Anyone else? No? OK. So the next question is, do our consumers suffer the same informational injury? For example, Professor Ben-Shahar said that no rational consumer would want to be burdened with privacy and data security choices. But if consumers desires are actually more diverse might some consumers actually be injured by the deprivation of that choice even if others are not. Do you want to?

OMRI BEN-SHAHAR: Sure. I want to correct that the understanding of what I said, or what I intended to say. Some consumers might want to be quote unquote, "burdened," with these choices. And I think few, if any, would want to make choices on all aspects of the consumer transaction. And there are many, many of them and there are many such transactions. There's just not enough time-- and people have studied that-- not enough time during the day to make these kinds of choices affirmatively. Some things you need to let go and not make a-- for some people

maybe the important thing is to choose are data privacy-- For others it might be other aspects of the deal. Maybe not necessarily that-- I don't want to say about what the ratios are because I haven't seen anything credible about that-- I mean people say that they want to but you know they don't behave as if they do. Any attempt to try to simplify the entirety of the privacy policies into something like nutrition labels. To make it possible for people to choose privacy like they choose food.

I'll just say in parentheses, I can't resist, there is no evidence that the nutrition labels changed people's diets in any meaningful way. But there is a strong perception that they do and that this is a model to choose. I tested that in my own work to try to create these kind of labels and to put people in a very nasty privacy setting where they should really worry. And to see whether they behave differently when they are treated to these really friendly warning boxes, as opposed to very cluttered privacy policies. And unfortunately found in a very large study no effect. So it adds to my concern that people generally view these kind of decisional aids as burdens.

DANIEL WOOD: OK. Katie?

KATIE MCINNIS: I would take Omri's burden and reclassify that as agency. A lot of consumers, as we've stated, don't feel like they have any control over their data and some of the only ways that they can even try to effectuate their choices are through these opt ins and opt outs. And in some cases we've even seen, as we saw in the recent courts article, sometimes those preferences aren't even followed by the company. So consumers really desire these tools. Yes, I think that the array of products that they interact with in daily life that really does tire the consumer out to make all these decisions. I would agree with you on that. But I also think that this is one of the few ways that you can really try to have some agency over the data that you're sometimes sharing without your permission.

And I would also emphasize that while for many consumers their privacy of what they're doing online or sharing with companies may not be a huge concern for them, members of commonly persecuted groups, or outlier groups, definitely have a huge interest in their privacy of the communications and actions online. Especially when we're looking at social organizers, or protesters, who are looking to effectuate change and the larger status quo, you definitely do have an interest in your privacy and your security online. And I think that if you didn't have that we'd see a huge chilling effect online. The NTIA did a study and found that since consumers feel so unsecured online they've actually change their practices online. Right? And that's even before net neutrality is taken away, before broadband privacy was taken away. So consumers are concerned, they just feel this lack of control. And it's up to us and to regulators to provide more control, more agency for these consumers, not less.

DANIEL WOOD: OK. I think we have time for one more question. And then we'll leave for a few minutes for last words from the panelists. How can industry and the FTC manage data mishaps? Audits? Who is the auditing agency question? For reference, my teenager weighs risks daily, yet often makes decisions based on what she'll get away with. Anybody want to take that?

KATIE MCINNIS: Unfortunately, the FTC has a retroactive authority to act on these matters except under a couple instances such as COPPA. My personal dream is for the FTC to have more

rule making powers so that we don't have to act after the fact, and after an injury has occurred in many cases. And I think that although we have a fragmented privacy regulatory environment in the US as we've seen under COPPA and other regulations, we've also mentioned some of the constraints on financial transactions. I think the consumers really desire more privacy and security over the data, and I wish that we had better-- although the FTC has had a great track record I'm not diminishing that-- I think that we do look for better regulations and better protections at the federal level especially since consumers have so few tools at hand.

DANIEL WOOD: OK. Anyone else?

CORA HAN: OK. Then let's move on to final thoughts. I will just go down the row and you could take about a minute to give us any of your concluding remarks. Let's start with Omri.

OMRI BEN-SHAHAR: Well, I'll say one thing. The ideas that I shared today were largely skeptical about what evidence do we have about injury? I don't want to sound, to deny the possibility, that good evidence would demonstrate that there is injury. I guess my main contribution I wanted to be a suggestion to the FTC that to the extent that you identify something that needs to be done, that choice of regulatory technique is not transparency, informed consent, give consumers control, improve their privacy policies, improve the format, give it in real time. All of these things have been tried endlessly in so many other areas including in privacy. And the performance of these tools is abysmal. They don't work. So if there is an injury to worry about, please let's not worry about it through the tools of transparency.

CORA HAN: Leigh?

LEIGH FREUND: Yeah. Thank you again for having us. I think I'd like to kind of focus us back on the purpose of the workshop here which was trying to define what informational injury is, and whether or not we can do anything about it either at the FTC or in other places. I think we heard wildly different opinions from experts on what was an injury on the last panel. And I want to really kind of focus on are we using data in a responsible way? Are we giving consumers power over their use of data? And how are we doing that in a way that mitigates both the risks and the benefits, and that not only to businesses benefit but consumers benefit? And I think weighing those risk factors and the benefits and the risks together. Injury is a really big word and it's very difficult to quantify. But I think we've gotten some insights today into how serious something needs to be in order to call it injury. And the rest of it we put guardrails around to make sure that people are using data responsibly in our industry.

CORA HAN: Thank you. Jennifer?

JENNIFER GLASGOW: I'd kind of summarize by saying, first of all I think when having these conversations you've got to deal with security issues in one bucket and you've got to deal with appropriate use of information and another bucket. I like to think of the appropriate use of information as introducing ethics into that. And we have lots of models in various industry sectors, legal sector. Many of you may be lawyers are familiar with ethical approaches to things. And I think that there is a play there that we can begin to adopt when it comes to various pieces

of information, as opposed to writing hard and fast rules about what you can and can't do. I agree with Leigh. Let's identify the really serious stuff and deal with it. But there's a lot in the grey.

The last thing I'll say is I think businesses are going to have to step up to doing more. This ties not just into the concept of security but maybe more importantly, into the concept of how they use information and/or how they share information, and what they've done to satisfy the expectation of the consumer, and what they've done to give choice to the consumer. Because that is the entity that will make those calls in the end. And I think we're going to have to take some things off the table from the choice scenario. I don't want to have to give 50 choices when I buy my connected car because that's how many sensors are in the car. I want maybe three or four choices, and the rest of it I want the car manufacturer to stand behind their decision to allow it or only use it in certain situations and so on. So I think we have to be cautious about giving consumers choices where there are varying differences in opinion and just helping them make the right choice when they're not.

CORA HAN: Bob?

BOB GOURLEY: OK. So first I'd say, hey I'm with her. Jennifer, I just really believe all that stuff. It's very important to consider both the security aspects and the inappropriate use and appropriate use of data aspects. It's very important. And she's also the one to first brought up the analytics, and the future of analytics, and the artificial intelligence is really going to be critically important. So many other things we didn't have time to discuss today. Maybe it's going to be on the next panel. But, things like tort law. Let's wait and see how these lawsuits around Equifax come out. And are there other cases where companies should be sued because of negligence? And what will the courts do to shape the future of this dialogue. I think it's a very important topic.

Also we didn't have time on this panel to really discuss best practices for businesses. There are so many of them out there that are captured and they need to be contextualized for businesses. But there's important best practices out there right now that more people need to know about. And the same for home. Us, people at home. Jennifer mentioned cars, of course, but you know cars, homes, all of your devices. What are the best practices for those? We didn't have time to talk about. We did have time to talk about the big guys who are really managing our data and are working hard to protect it. GAFA. And I said, what would GAFA do? We need to keep watching that. Those are my concluding thoughts.

CORA HAN: Thank you. And Katie, for the last word.

KATIE MCINNIS: Thank you for having us on this panel. I found it very interesting, and it was also great to meet many of you in person. I just wanted to take a page out of Bob's book and mention that there's one thing that we didn't talk about which is another injury to consumers, which is a loss of consumer power. If tons of information is being collected about me, with or without my knowledge, and that leads to first party price discrimination, that is an injury to consumers. And that's one that I think we're overlooking and haven't paid enough attention to at this time.

I also want to emphasize that Consumers Union and Consumer Reports, which is the same thing, is really looking to try and provide consumers with more agency and more ability in the marketplace to really decide what kind of products and services you want to use. Based not only on the services that they provide, but also based on the security and privacy of those services. And we hope that we can help change the marketplace so it is easier for consumers. And so that we don't have to get tired out by all these different disclosures, even though I personally see that more of agency issue than a burden. And I want to point you all to the security planner from the University of Toronto Citizen Lab, which can help each and every one of you effectuate some privacy and data security protections while online. It can be tailored to you. And thank you Cora and Dan for organizing this panel.

CORA HAN: Great. Thank you. Please join me in thanking our panelists.

[APPLAUSE]

It was a great discussion. And we will be on break until 3:30, when our last panel on measuring injury will begin.