FTC Fall Technology Series: Smart TV Workshop
December 7, 2016
Segment 2
Transcript

MEGAN COX: Well, welcome back. Thanks for attending our workshop here today. And for the second panel this afternoon, on consumer understanding and regulatory framework, I have with me Dr. Serge Egelman with the Berkeley Laboratory for Usable and Experimental Security. I'll go down the line here, I guess. We have Emmett O'Keefe with Data and Marketing Association, Dallas Harris with Public Knowledge, Claire Garland with Epic, and Maria Rerecich with Consumer Reports.

Thank you all for joining us here this afternoon. And I want to remind everybody, we will take questions via Twitter. If you want to tweet them at us, we can take them at #smartTVFTC. And we'll continue to have Matt circulating, if there are other questions from the audience.

So to begin the afternoon's discussion about consumer understanding, we have Serge with us to present on some of the research that he's been doing lately, I guess, in the last few weeks. We heard from panel one this morning, about how a large amount of data is generated by serving content through smart devices and applications, and entertainment preferences are identifiable, and that data is used to identify trends and support content in analytics and advertising.

So Serge, what has your research shown above what data consumers expect to be collected and the parties that data is expected to be shared with? Who do consumers think that the data is shared with? And is this sharing acceptable to them?

DR. SERGE EGELMAN: Yes, those are all very good questions. And I have some slides on this. So my research is basically centered on how people make decisions about privacy and security and then using data from these experiments to try and come up with user- centered designs for new interfaces, to give people more control over privacy and security. So previously, we had been doing some research, over the past couple of years, looking at mobile devices and also wearables, with an eye towards ubiquitous data capture. So devices that you carry around that have lots of different types of sensors, which could in theory be continuously capturing data about the users.

So recently, we came up with a study to look at wearables in particular, and we were interested in how people perceive the sensitivity about different types of data, as well as how the recipients of that data might drive some of those concerns. So we did this online experiment where we gave people a bunch of different scenarios. We combined 72 different data types-- such as photos from your wearable device or audio picked up from your wearable device-- with four different recipients. The recipients were servers with no human looking at the data, the general public, co-workers, and friends. We had a little under 2,000 internet users participate. And from these almost 300 different scenarios, we just randomly selected five or so for each participant.

This is an example of one of the scenarios. We made up a wearable device. We didn't want to prime people to existing concerns with things like Google Glass, which might bias some of their

responses. And so we made up this device, the Cubetastic 3000. Before they started the survey, we came up with a bunch of use cases and possible benefits for why people might want a wearable device. And then we presented them with the scenarios.

So in this case, one of the scenarios is how would you feel if an app on your Cubetastic 3000 learned when, how, and how much you exercise and shared that with your work contacts? So here the data type is your exercise routine. The recipient is work contacts. And then we had people just rate these on a scale. And the point of this was so that we could come up with relative levels of concern, as a function of the data type and recipient.

Basically what we found was that there are significantly lower levels of concern when sharing with non-humans. So by and large, when people were told that this would go to some server that would calculate-- you would use machine learning, but no human would ever view the data, by and large people were OK with this, at least more so than when there was a human recipient. The corollary to that was we actually didn't really see any difference between the different types of human recipients. People were more concerned with whether a human was viewing it, rather than which human was viewing the data.

We also found that data types that we hypothesized would be sensitive-- like video or audio captured within the home environment, say the same types of data that a smart TV or smart entertainment center might be able to capture-- were perceived as the riskiest, similar to things that might incur financial risks, such as disclosing banking information or credit card numbers. The opposite end of the spectrum, with things that are perceived as already being publicly observable, such as demographic data-- so if you go out in public, people can pretty accurately make assumptions about your age, gender, and so forth. People tend to view those types of publicly observable data types as less sensitive and were pretty open to sharing those types of things.

Moving on to smart TVs, very recently-- literally, like two weeks ago-- we conducted a survey specifically focused on the types of data that is either currently being captured by smart TVs or could be captured in the future. So we gave people a scenario around one of these data types. We had six different data types we presented people with-- voice recognition, personalized recommendations, gesture recognition, user recognition-- maybe for personalization purposes-- presence detection, and the ability to run third party apps were the six different scenarios that we focused on.

So here's another example. So for each one, we wanted to prime people to the possible benefits of each scenario, without immediately delving into privacy risks. Because if you just start asking people about the privacy risk without explaining possible benefits, then obviously the data is going to be kind of biased.

So we presented a scenario. Here we have personalized recommendations, saying why people might be benefiting from the personalized recommendations. And then we asked them how interested they are in this feature. And then afterwards, we went into questions about how the data might be used, and who they believe it might be shared with and so forth.

We recruited about 600 participants from Amazon Mechanical Turk, which previous work has shown is relatively representative of the US online population. We had a good balance of gender and good distribution of age.

So in terms of what we found in terms of privacy concerns, the first thing that we asked about is when data is collected for this purpose on the smart TV, do they believe that the data stays on the device, or is it being uploaded to some other server somewhere. And I'll preface this with the question about malware I did not include in this analysis. That's a separate thing, which I'm not really going to get into today, due to time.

So by and large, people perceived that the data would not be leaving the device. So here this shows blue is the people who outright said no, the data does not leave the device. Red is people who said they're unsure.

And so in most cases, the people who believed the data would be leaving the device are in the minority. So in the case of voice recognition, we know that most of the devices that are doing-- many of the devices that are doing voice recognition upload it to the cloud. So the fact that around 70% didn't believe that this was happening is a little concerning.

The next question that we looked at was whether they believed data would be used for other purposes. And so we found that this was strongly correlated with whether they believed the data would be leaving the device or not. So in the case of recording audio for voice recognition, the number who said that either yes, they definitely believe it will be used for other purposes or those who were unsure were also around 70%.

And it drops off from there. It seems there's a big contrast between video that's captured maybe for doing user recognition or gesture recognition. Fewer people believe that this would be used for other purposes.

The other thing that was really concerning is that many people presumed that there were existing legal protections that would prevent the data from being used for other purposes or even from being shared with other third parties. So we asked people if there were laws or regulations that exist that prevent the sharing of any data collected from the smart TV within their home. And we found that this was also-- belief that strong privacy laws exist that prevent this from happening was strongly correlated with whether they believed data would be used for other purposes. Rather, inversely correlated, so people who said that data would not be used for other purposes by and large believe that there were strong privacy laws that prevented this from happening.

And in many cases, this is simply untrue. Obviously there are sector-by-sector privacy regulations in the US. But there isn't any uniform regulation that would outright prevent any sharing of data collected from these devices.

So here's a sampling of quotes. Some of the people said things like existing privacy laws prevent any sharing of data without permission. There are people that had very vague notions of privacy laws, so many people said, the privacy law or collection of privacy laws prevent all of the practices that we were asking about in the survey.

Also there was a lot of cynicism on the other side. So there were many people who said that privacy laws may exist. But in practice, they're useless. Because either the terms of use will allow the recipients of the data to override the privacy law, or there's just no enforcement, and therefore it doesn't matter if there's a law or not.

And so the last chart here shows the different recipients that we asked about. So we asked people two questions-- whether they believed it was likely that these recipients would be receiving data collected from their smart TVs, as well as whether or not this was acceptable to them. And what's interesting here is that there's a big contrast between what people believe is happening in terms of who data is shared with, and whether they say it's actually acceptable to them.

It's not necessarily clear whether we should be setting policy around expectations. So Helen Nissenbaum the philosopher has written a lot about this, in terms of examining privacy-- not in terms of preferences, which has historically been done-- but also in terms of expectations and awareness and trade-offs. So the fact that people say this is likely or unacceptable, it's not clear how we should actually interpret that.

So the main takeaways from this, though, are that many people believe that privacy laws exist and are protecting them in cases where they may not be. And also, others understand that data can be shared, are opposed to it, but don't believe they can actually do anything about it. This sort of goes to Skinner's notion of learned helplessness, which has also been discussed a bit in the privacy literature. I guess I'll just leave it at that. MEGAN COX: Thank you Serge. That was an interesting presentation with great insights. I thought next we'd go to Claire Garland with Epic, to ask you from your perspective in your work there, what do you see as consumer understanding and what data is being generated and collected by these different entities in the smart TV data ecosystem. And do you see potential harms and benefits that can come from that, and where those lie right now?

CLAIRE GARTLAND: Thanks so much Megan. And thanks for hosting this workshop and for inviting me to participate. So I think that Serge's excellent research really shows that consumers are not aware of what's going on, how data is collected, used, and disclosed. And I think that consumers really are unaware that their smart TV is actually watching them back, as they watch the TV.

And I think a lot of this has to do with the fact that TV devices themselves are really intermediaries. And so the fact that this intermediary device is recording your interactions with other applications is really inconsistent with the context. The consumer isn't trying to connect with the TV. They're simply using that TV as a platform to connect with other service providers, whether it's Netflix or live TV, that sort of thing. And so I think that, again, is inconsistent with the context of the interaction.

I think another issue where consumers don't understand, and this is supported by Serge's research, is the really complex ecosystem that comes into play when smart TVs are involved. There are many actors with access to their personal data. And they all have access to viewing habits. But these relationships may not be clear to consumers.

I think it's also interesting to think about the variety of actors that are at a given moment collecting the information from a TV. So let's say you're watching Netflix through Apple TV, which is hooked up to your smart TV. All of those actors are collecting this information and sharing it, disclosing it, to unidentified third parties.

So even if consumers wanted to learn where that's being disclosed and how those actors may in turn use and disclose that data, it's very hard for them to figure that out. Because privacy policies largely don't explain this. So I think in some, in terms of the understanding of data generation and collection, consumers are really left in the dark. And even if they were to try to seek out this information by reading privacy policies of the various actors in this, they'd still largely be left in the dark.

So in terms of harms and benefits that come from this sort of data collection and retention and disclosure, this smart TV data ecosystem-- so I think in the first panel, we did hear quite a bit about the benefits to consumers. Certainly recommended content when you go on to Netflix. And let's say I watch Stranger Things and they recommended another sci-fi show or something. That can be a benefit to consumers.

But on the other hand, there are a lot of revealing, intimate things that can be gathered from users viewing data. I think a lot of us have heard the cliche, you are what you watch. And I think that is really true.

And in addition to showing what a viewer's sophistication is-- their interest, their level of education, that sort of thing-- it also shows revealing information about consumer's lifestyle, whether they are up until 3 AM watching online shopping channels, or whether they've suddenly started watching a lot of TV during the day, which may indicate that they've recently become unemployed. So really there's a variety of issues here.

And again, we saw that consumers are concerned about who gets information. And you can imagine a circumstance where perhaps insurers-- who are beginning to partner more and more with connected home device suppliers-- could potentially be obtaining that information, or employers, or other people who are using that generated information to make eligibility decisions about you. So there are a variety of risks.

And as we recognize, this industry is really in its early stages. And I think it's important to be aware of the ways that viewing data can be used in harmful ways against Americans. And a statistic that I think is really interesting that was revealed in Joseph Turow's research study he presented at last year's Privacy Con is that 72% of Americans reject the idea that what companies know about me from my behavior online cannot hurt me. So consumers are largely aware that information that's either directly generated or inferred from information that's directly generated can be used in ways to discriminate about them or to make other negative inferences about them.

And I'm glad that we're having this conversation. It's something that I hope everyone is able to keep in mind, as this industry progresses.

MEGAN COX: Thank you for outlining those risks. I think those are some challenges and some pitfalls that need to be discussed. But to follow up on some of the benefits that this information collection can do, Dallas, I was wondering if you could talk about how on the first panel we heard how more niche audiences can be brought into the fold and served with more ads and content, how better metrics for that can allow these communities to be reached with some of the specific ads in content, and how it can be more inclusive for all kinds of campaigns and bring more. So can you speak to that benefit and some of the privacy protective ways that it might be brought forward?

DALLAS HARRIS: Sure. So I agree wholeheartedly with everything that Claire said. And I think that the benefits are clear. Nobody likes ads, so if we could get less of them, that would actually be relevant to something we might want to buy, thumbs up.

But I think the harm can be easily summed up in something that Serge said. It's very illustrative of the problem, is this idea that when we think about privacy, we're learning about the idea of learned helplessness. And the harm is that consumers are starting to feel helpless about having control over their own data.

So I would say it's public knowledge's position that benefits are clear. Consumers can get cheaper services. Hopefully maybe even one day, the whole internet could be free if it was all ad supported.

The problem is when consumers don't have the option to participate in a meaningful way and aren't informed about those benefits and the potential risks that come along with sharing that information. And to your point about particularly niche markets-- low income, minority communities-- these are communities that are already disenfranchised. And so the risk to them is also a bit greater.

MEGAN COX: Thank you, that's an interesting point. And I think that kind of tees up the next section we're hoping to shift gears and talk about, which is the legal landscape of smart TV world here. And before I get to that topic, we did have a question passed up about the Twitter handle for today or the hashtag. And I just want to remind everybody it's #smartTVFTC and that the slides of it will be available on our website. So if we pass through them quickly, they will be up on the website.

And with that, I would like to ask Emmett if he could speak to both how he sees laws that have been tossed about a little bit earlier. In Justin's presentation, they were mentioned, section five of the FTC Act, the Children's Online Privacy Protection Act, the VPPA and the Cable Act, those have all been referenced to today. So could you speak a little bit to what protections you see those providing in this space, and where there might be gaps, and if self-regulatory efforts might be moving into this space in a bigger way?

EMMETT O'KEEFE: Sure. And let me start out by first saying thank you for having us here today. It's nice to be up here with this illustrious panel.

I am [INAUDIBLE] for the Data and Marketing Association. And at DMA, we're constantly looking into new and innovative uses of data and how those interact with existing laws and self-regulatory programs. To that end, earlier this year, we began examining what we call the next generation TV ecosystem and developing a white paper for our DMA members-- that will actually be released this week-- that looks into the existing legal and regulatory landscape in this area.

And what we found is that it depends. You know, it's part of it. We look at all of the laws that were mentioned.

We examined-- certainly section five will apply, subject to the limits of the FTC's jurisdiction, of course. But it will apply to unfair or deceptive acts or practices made by providers within the ecosystem.

The Cable Act will apply to the provision of cable services by cable operators, as it always has, within the jurisdiction of that statute. And then COPPA and VPPA are very fact specific, but they're out there in something that all the service providers-- all the next generation television service providers will have to take into account.

But let me, if I may, step back and say as we discussed this legal landscape, part of the question about what is this legal landscape almost comes with the presumption that something needs to be done. When, yes, we have all these laws out there and they apply, depending on the facts and circumstances of the case. But let's step back and just caution that when we heard on the first panel today-- we heard a lot about convergence. And we heard about how the internet is converging with the traditional linear TV market. And that's great.

And they talked a lot about the benefits to consumers. And they also talked about the need to responsibly use data to use those products and find new ways to bring those benefits to consumers with real notice, choice, and control mechanisms. And those are all pursuant to some of the laws that we just went through.

But let's be careful here not to jump to a conclusion that we need a whole new set of anything, when what we're seeing here is convergence, where basically many of the apps and services that people have been using for many, many years are simply migrating to a new device. Many of these apps and services-- all of them of a certain age-- started on the desktop. They went to the laptop, they went to the tablet and the set-top box.

And now they're migrating to-- now as technology evolves and on the hardware side, it is easier to have it migrate directly to the television set. And that's wonderful for consumers. This is just a natural extension of those online services that people have been experiencing for many, many years.

And so the question is do we need to presume that something needs to be done, when we already have all these laws out there? Nevertheless, DMA is a big proponent of self-regulation. And we've had our ethical guidelines to business practices for setting best practices and standards for what are ethical business practices in the marketing space for many, many years, many decades,

in fact. And we're, in fact, going through-- those have been periodically updated over the years, and we're going through another periodic update. And this is one of the topics, along with other internet of things topics, that are on the table for discussion.

So right in line with all of the comments about how this is early stages and nascent stages and early days for this environment, that is we've spent the better part of this year refreshing our guidelines a bit. And phase two is to look into specific business models and practices. And that's how we'll be spending our time in the coming months.

MEGAN COX: So when you're refreshing your guidelines, does it apply to your membership being all those involved in marketing practices? Or are the guidelines-- can you speak to what parties that would apply to?

EMMETT O'KEEFE: Our guidelines are written for our members. But they are applied universally across the industry. It's a complaint-driven process. And we enforce them, whether it involves a member or not.

MEGAN COX: OK, thank you, that's helpful. So I think that Claire's work at Epic has evolved a little bit of briefing around the VPPA on various cases. Could you speak to how you see that law in particular applying to these spaces, in both streaming services and smart televisions and devices?

CLAIRE GARTLAND: So there's been a lot of interesting developments in case law recently, applying VPPA. And I think they sort of fall into three buckets, in terms of the specific issues that are dealt with. So one is what qualifies, who qualifies as a videotape service provider.

And there is a decision in In Re Hulu that affirmatively stated that Hulu is a videotape service provider. And this was determined in recognition of Congress's intent to protect the confidentiality of individuals' viewing preferences, regardless of the business model or media format involved. So it's pretty clear that Hulu, Netflix, these types of online video services fall into that VTSP videotape service provider category.

Now as I think was mentioned earlier, there is some ongoing litigation against Visio, the smart TV manufacturer. And that's been focusing quite a bit on whether smart TVs qualify as videotape service providers. So unfortunately, I think the VPPA is sort of an example of shortcomings when Congress legislates in a really technology-specific way as opposed to technology-neutral.

But it's important that our interpretations of the statute really reflect the underlying intent of Congress, which is to protect the privacy of what people view in the privacy of their own homes. So treating smart TVs when they handle the exact same information that Hulu, that a cable company is handling, simply because they're not falling in line with language from the 1980s, I think would really conflict with Congress's intent here. So that remains to be seen. There hasn't been any affirmative rulings from courts, to my knowledge, applying the VTSP definition to actual smart TVs.

So that's the first bucket. The second is whether a consumer is a subscriber. So it has to be a consumer's video viewing history that is disclosed to a third party.

And we've seen a variety of conflicting messages here from courts. Some have said, for example, in a case against Cartoon Network, that when someone downloads a free app, they're not a subscriber. And they really focused on the lack of monetary exchange there and the user's ability to just delete the app whenever they want.

But on the other hand, in a case against Gannett's satellite info, the first circuit found that by providing personal data and having that data collection collected, that constitutes payment. So therefore, the user of an app is, in fact, a consumer, for purposes of the statute. And I think that is more consistent with the reality of the way that today's modern marketplace works.

Many people have heard the phrase, if you're not paying for the product, you are a product. And you're paying with your personal information. So I think that that interpretation, regardless of whether there was a monetary exchange, is more consistent with understanding who a consumer is for these purposes.

Now I think sort of the biggest and most important challenge that courts are facing is what constitutes personally identifiable information in this space-- and not just for the purposes of VPPA but really across the board. Courts are unfortunately applying 20th century definitions of PII to 21st century technologies. And this is doing a lot of harm, in a variety of contexts.

We heard in the previous panel, and as we hear industry talk about what's PII. They're very consistent in making clear that IP addresses and device identifiers are non-PII. We hear this consistently across the board.

But that's just not the case. You know, if my name is John Smith, that doesn't really tell you a whole lot about who I am or which of the thousands of John Smiths I am. But if I am Mac address a very specific, unique number, that is unique to my phone or unique to my television or my unique IP address, that is a lot more identifying, when it comes to locating a specific consumer.

So in terms of how this has been interpreted by courts applying the VPPA, there's been some cases, unfortunately, that have misunderstood 21st century PII. But there has been decisions that have recognized that for example unique Android ID and GPS coordinates are PII.

And this is really more consistent, as well with our counterparts in the EU. The EU Court of Justice recently determined that both dynamic and static IP addresses are PIIs. So that is the law there now. And that really is, again, more reflective of 21st century technologies.

MEGAN COX: And to go off of that, I think that we've heard mentioned earlier of the Children's Online Privacy Protection Act that does include persistent identifiers in the definition of personal information. And so it can be implicated in some of these settings. Dallas, did you have thoughts to add about how you see these laws apply in this--

DALLAS HARRIS: Sure, so in particular, I wanted to point out something related to COPPA and then the cable Privacy Act, as well. Interesting about COPPA, there are two things. It applies to a website or online service.

So the first question we have to ask, is the smart TV a website or online service? Let's say we get over that hurdle and say it's an online service, it's connected, you have apps. OK, great. But it has to be a website or online service directed to children. And I think it's very hard to argue that smart TVs are a website or online service specifically directed to children.

Now here's where the problem comes. I mean, I'm sure none of you spoil your children. But your child may have a smart TV in their room. And to Claire's point, if you can get the identified Mac address and say, you know what, we're fairly certain that this belongs to a child. It's only on after 3:30 PM for a certain amount of time. It only watches, you know, Nickelodeon and certain-- you can make these inferences from information that in itself is not considered necessarily sensitive.

We might end up with a situation here where there's a slight loophole around COPPA, where you can send direct advertisements to that device, without saying, well, I know for sure I'm marketing to children or that I have actual knowledge that there is a child here. So there's an issue with COPPA there when it comes to smart TVs and something that we're going to have to think about.

And then the other thing I implore everybody to kind of think about, especially the FTC, is when it comes to the Cable Privacy Act, this is something that both the FTC and the FCC have joint jurisdiction over. And with smart TVs, the FTC and the FCC are going to have to work together, I think very closely, to try and protect consumers in this space. Neither agency has complete jurisdiction over the Cable Privacy Act.

And then the last thing I'll say, especially when it comes to the Cable Privacy Act, the FCC has not made any explicit rules to enforce the Cable Privacy Act. And so they've been relying mostly upon consumers' ability to take companies to court on their own. That stops when it comes to arbitration clauses and mandatory arbitration clauses and the ubiquitous use of them. And so when it comes to the Cable Privacy Act and smart TVs, when you see these terms of service, the FTC and FCC are really going to have to work together. And maybe we might need some rules to actually be put in place to protect consumers properly.

MEGAN COX: Thank you for those insights. Emmett, did you want to respond at all?

EMMETT O'KEEFE: Well, not to respond but just to comment, is that all these concerns are well-founded. And I respect the sentiment behind them. But we have to ask from a policy perspective, what is different here? We're just talking about a different device.

All of these same services that are being employed on the television now have been employed for years in everyone's pockets and on tablets and certainly on laptops and desktops and the like. And so if there are gaps, maybe they could be addressed. But I don't see where the gaps are right now, in that we're really just talking about a different hardware application-- application meaning the dumb word, not the specific word.

MEGAN COX: And Serge, you wanted to comment?

DR. SERGE EGELMAN: Yeah, I guess I kind of want to tie this into something that Emmett said earlier. There isn't much different here, in that self-regulation in the privacy space has been an abject failure. So everyone pretty much agrees the website privacy policies are completely incomprehensible and are often so ambiguous that most people don't understand what's being collected and who's who it's being shared with.

And now that that's moving into the TV space, it's not any different. Because as we've seen, consumers then don't have any idea of what's being captured on their TV and who it's being shared with. I'm not saying that we need new regulations to regulate how data is shared necessarily.

But we do need to do much better in terms of disclosure. I'm not, with regard to privacy, personally, I don't think we should be prescriptive in terms of necessarily what practices should and should be conducted. But there should be informed consent.

And right now we're not getting that. We weren't getting that really before. And we're not getting that now that we've moved into the home on the TV.

MEGAN COX: And I think--

EMMETT O'KEEFE: If I may, I have to disagree with the assertion. The assertion is that self-regulation hasn't been working, when self-regulation has been cited multiple times by our government agencies as being quite successful. And we have a robust system on the web side for notice, choice, and control. That is kind of the gold standard. And if we need more attention to this in this space, that's exactly what DMA and I heard NAI saying that they're going to look into.

DR. SERGE EGELMAN: I guess it depends on how you define successful. Because all of the literature on consumer understanding of privacy policies has shown that people don't understand privacy policies. And sure, it's been successful from the company's perspective, in terms of staving of regulation. But in terms of the consumer perspective, I don't think it's been successful. And the data bears that out.

MEGAN COX: And I think this would be a great time to talk about what Consumer Unions new project is with-- or Consumer Reports rather-- where they're working on disclosures and what consumers are able to find out about different products. So as these new methods of tracking come into existence and new products, and how to best disseminate and message to consumers what choices they have, what controls they have. So Consumer Reports has been working on a framework related to privacy practices among the different devices, including smart televisions. So Maria, can you talk a bit about this work and your thoughts on what consumers are told about data privacy practices?

MARIA RERECICH: Sure. So at Consumer Reports, we're currently exploring how as a consumer product testing organization we can evaluate the privacy security and data practices of

a product and incorporate that into our testing protocols and our product ratings. We are currently working with several partners. And we're working toward developing an initial version of a proposed test standard that will take into account these factors, these different type of aspects.

It includes concepts such as is it safe, is it private. Safety is about security, it's about encryption, it's about can you update the software for security patches, things of that nature. Is it private includes things like the actual permissions that are granted, the data sharing that happens, and the disclosures and things of that nature as well.

We're currently conducting pilot tests that we're wrapping up for several products, including smart TVs. And we're doing that to exercise the standard as we're putting it together and try to make sure that it holds together, and that it makes sense at least for a variety of different products. So we're doing that.

And the idea here is that whether self-regulation has been a failure, as Serge says, or not, as Emmett says, we feel with some sort of test standard that we can use and we can bring to bear to this, we could say these products are better for the consumer, these products are not as good for the consumer. And then in this way, we could influence manufacturers and service providers, and that we can actually move the marketplace, by having some sort of concrete way to say, this is better than this one. And we think that manufacturers and service providers will move to that. The marketplace will move because of that. So that's what we're working on.

MEGAN COX: Thank you. So the timeline on that is that you hope to launch it early in the next year, is that right?

MARIA RERECICH: Yes, early in next year, we're heading into PrivacyCon, hopefully for that.

MEGAN COX: And that will seek comments. So what is the timeline on which consumers can expect to see this more at work in the private sector?

MARIA RERECICH: Well, I think it will take-- it needs to-- launching it right before PrivacyCon and discuss it at PrivacyCon, We'll be looking for comments from everybody to make it better. Something like that is a living document and needs to keep moving and progressing as the technology changes, as practices change, as things get better. And we'll try to do the best we can to start incorporating into that into some evaluations of products as we go.

MEGAN COX: Great, thank you. And so with those types of evaluations of disclosures, I think it's an interesting time to ask Dallas to chime in on what your analysis of certain disclosures have been. Particularly, we've seen some public companies that make certain disclosures in one set of documents regarding-- to their investors, or if they're marketing their products and services to certain businesses about what they're able to do, their capabilities-- and then with their consumer disclosures might be a different set of information or messaged in a different way. Can you speak to what you've found in your work on that?

DALLAS HARRIS: Sure, so we're at the FTC. So the question is all about the gap between what the companies are saying and then what they're actually doing. And if-- I don't intend to pick on anybody, but Comcast is such an easy target--

[LAUGHTER]

If you just think about it for a second, Comcast owns this technology, which is actually capable of inserting personalized content into network streams, including advertising messages tailored for specific individuals. So they're doing this without using your PII-- personally identifiable information. Yet they can still target you personally.

Comcast also owns Visible World, which uses data from millions of smart TVs. The data includes income, ethnicity, education level, what kind of car you drive. And Visible World has an addressable footprint of about three million homes.

To take it another level further, Visible World then also controls AudienceXpress. AudienceXpress works with ComScore, who was on the first panel. And their data analysis includes actual product purchasing behavior, credit card spending data, and multi-screen activities of consumers. One of their executives said, "No one in the TV industry has ever combined online deal with TV viewership data." Great for them, right.

Now I'm paraphrasing here a little bit. But if you pull up their privacy policy, Comcast privacy policy says something similar to this. We will use your data for things like advertising. We may combine that information with third parties. Those third parties may combine that information with some aggregate or sometimes deaggregated demographic information.

I'm not quite sure that that paragraph quite explains the level of complexity that Comcast is involved in data collection. Not just Comcast, but the parties that they own, and then the partners that they work with beneath that.

So it's our opinion that there is a very large gap between what is actually being said and what Comcast knows for a fact it's doing and it is capable of doing. And again, I don't mean to single out Comcast necessarily. But you know-- and I am sympathetic to the challenge. You can't have these extremely long privacy policies that consumers are going to glaze over, which they're doing already.

But there's got to be a better way to explain to people, listen, we're not using your PII to advertise to you. But we still know who you are.

MEGAN COX: And Maria, do you think that your metrics will be able to capture that and convey to consumers what kind of privacy policies and behavior of data practices that you're seeing?

MARIA RERECICH: Yeah, I think it should touch upon those aspects. Because, again, what we want to make sure is that for the consumer that there's transparency, that they have control over their data, they have choice. These are the things that are important.

When it comes to the actual privacy policies, even though they're there-- if you just look at a smart TV now. There are smart TVs, we've seen a privacy policy was 47 screens. You bring home your new 65-inch TV.

You're ready, you hook it up. You turn it on, you select your Wi-Fi network, you put in your password. And you're ready to-- oh, you go there's a screen.

So you need to see these screens. Like I said, 47 screens of a privacy policy. Another TV had 18 sections in the terms of use, 11 sections in the privacy policy, and another screen with three riders for various services that are provided.

People are clicking I accept all. They're not reading those. That's not beneficial. Yes, the letter of the law, they gave a privacy policy. They disclosed. But that's not really disclosure.

You also have the case of even if they did read it, is it understandable. There's a privacy policy we saw, and it said, the wording was, "We may use automatic content recognition, ACR, and other technologies to capture the information." That's the only explanation it gives about what automatic content recognition is.

And as was said in the first panel, people don't understand that. They don't know. But it's there. It's disclosed. But it's not understandable to the consumer. And that's not transparent.

MEGAN COX: So Emmett, did you want to speak to-- sorry.

EMMETT O'KEEFE: If I may jump in, I don't want to speak to-- I know I'm not familiar with any of the specifics of what was just described. But I feel like we're having a panel discussion about the golden age of television and all the successes and benefits that this golden age of kind of interconnected TV is bringing to consumers. We had lots and lots of conversation about it in the first panel. You know, recommendations, and The Gilmore Girls coming back and Arrested Development coming back.

And all of this-- or much of it being done by the same internet providers-- internet, whether it be app or platform or whatever-- that people are quite familiar with in the regular online world. And then we're supposed to be talking about the specific application to what's changed in the smart TV world. And I still rhetorically, not so rhetorically, ask the question, what has changed. I mean, these are all many of the same services, and they're just being applied to a different screen.

The conversation that we just had about privacy policies and the like, that's a much broader discussion than the one we're here to have today. And we can come back another time, or we could have it now, or we could come back another time and have that broader discussion about what should be in a privacy policy, what shouldn't be in a privacy policy, etc. but I feel like we're getting pretty far afield from anything that's specifically pertinent to the interconnected next generation television services.

DR. SERGE EGELMAN: Yes, so here's something that's changed. I mean, people don't expect their TVs to be recording their viewing habits. They don't expect their TVs-- they don't expect

TVs to be recording audio within the home. They don't expect their TVs to be recording video in their home. That's what's changed.

CLAIRE GARTLAND: I think, again, going back to the idea that these TVs are really intermediaries. They're platforms to access other content. And that's what's different here as well.

You know, if your computer was logging your every keystroke and recording everywhere you went, any sounds or your images and then sending them back to HP or Dell, we would all be up in arms. That would be really concerning.

EMMETT O'KEEFE: Except with respect, this device that everybody has in their pocket is an intermediary for content. In the same way as those monitors are over there. It's very-- they're just different in size and shape.

MEGAN COX: So is it your idea that perhaps more education needs to be around how to treat TV manufacturers, and what to expect about their place in the data ecosystem? That it's another device that's part of a device graph, if you will?

EMMETT O'KEEFE: I think it's always worth looking at how consumers can benefit from additional education. But I think we should give consumers more credit than they're getting. People, again, I'm sorry to belabor the point. But people have been watching the same-- we all have apps on our phones. And now those same apps are on a larger screen. I intuitively know, I understand-- not intuitively, I understand how those apps work. I understand--

CLAIRE GARTLAND: Most consumers don't.

DR. SERGE EGELMAN: Yeah, and people are equally concerned about what their smartphones are capturing about them, and what's happening with that data.

MARIA RERECICH: It's an issue of consumer expectation.

EMMETT O'KEEFE: But five years ago, did we have a big uproar over smartphones?

DR. SERGE EGELMAN: Yes, yes we did. Yes, and it's ongoing. We still do.

CLAIRE GARTLAND: The issues we're raising apply across the board. But that doesn't mean we should ignore them when they apply to TVs, which by the way, are incredibly expensive consumer devices that people invest a lot of money in. They don't expect that to somehow further be subsidized by profits to the manufacturer from advertising.

MEGAN COX: And we did get one question submitted, I think to Claire, specifically. You had mentioned earlier about persistent identifiers, and how these might bring about specific harms, that you can be tracked with specificity over devices. So could you clarify your position about what kind of concern there should be around that, and what around I think Mac addresses and other permanent identifiers that you mentioned?

CLAIRE GARTLAND: My point there is that IP addresses and Mac addresses, any kind of unique, persistent identifier is the 21st century version of your name and address. That's how advertisers track you across the internet. And that's how they contact you. They contact you by sending something to this IP address, essentially.

And so to continually refer to these things as not personally identifiable is not only inaccurate, it's also really misleading to consumers. Every privacy policy I read says and non-personally identifiable information, such as IP addresses. I mean, their industry is really-- go through a lot of effort to instill in consumers somehow that IP addresses don't allow them to uniquely identify you and uniquely communicate with you. So in terms of harms, I think it's misleading to think that these unique person identifiers are not just as, if not more, personally identifying than the sort of traditional analog versions of identifiers.

DALLAS HARRIS: I'm actually going to do something I rarely do and stick up for companies here. That's part of the problem with our privacy laws, is the idea that personally identifiable information is clearly defined in the Cable Privacy Act, in COPPA, in all the separate, sector-specific laws that we have in HIPAA. And right now, the definition does not include IP address.

CLAIRE GARTLAND: It doesn't specifically say IP address in a list.

DALLAS HARRIS: Right, no it doesn't. But they are not being misleading, necessarily, by saying when we say we're not using personally identifiable information like your IP address. I think that's something-- you know, this is a reason why we need Congress to actually go back and think about how these laws apply in the 21st century. And that's a glaring loophole, I think, that you've pointed out there.

CLAIRE GARTLAND: And just by looking at the plain language of these statutes. VPPA and many others say when they're defining PII, they say the word, includes, which by definition, by implication, means that this list is not a complete list of all things that could be PII. And as data science becomes more sophisticated, more things become PII. Because it's easier and easier to link a piece of information that maybe 20 or 30 years ago wouldn't have been PII.

And you know, Congress, I think in a way understood that, by saying, "includes," not "this is a complete list of PII for all time, it's just these pieces of information." They provided examples not a closed list.

MEGAN COX: And I think, to move the conversation forward a bit from disclosures of where different methods for disclosing and screen size and that just in time notices, it is a robust discussion that needs to be had and that we've had a separate workshop on. So I know that there's a lot to drill down there with what is best practice.

But to talk a little bit about what goes in hand with disclosures is choice-- consumer choice, consumer control. So should consumers be given control over the data collection by first and third parties on smart televisions? We do know, as Claire said, that TVs can be very expensive. It's an investment, you have it in your home. There's a historic understanding, perhaps, with what a television does, a television manufacturer.

So how is that expectation dealt with? And is there given control, then, to the consumers about whether they can opt in to get the personal recommendations? I know in the earlier panel, Jane Clarke mentioned that she thinks it's like voting and that contributing with your data to these data streams to enable smarter algorithms, to provide smarter recommendations and personalization, to pick up on a movie where you are on a different device.

So I think Maria, I think you've considered this in some of the testing of products you've done. What has your work found?

MARIA RERECICH: Yes, so it's good to say that people should always opt into it. They need to have the information to be able to do that. It needs to be transparent to them what they're agreeing to do.

If they do that, then they can freely decide yes, it's worth it to me. I get a benefit from giving my data. And the whole idea here is that the consumer should get a benefit that is commensurate to the value that is going out to the vendors. As long as they're getting value for it, they can make that decision that they want to give that data.

What we found by looking at whether there were controls and choice on that is that the controls are usually there in the screens-- those 47 screens that you're going through. You do have the control-- there's a question whether it should always be an opt-out versus an opt-in or vice versa. But those controls are buried in menus. They're sometimes difficult to find. And they're sometimes not described or named.

So one example is the automatic-- the content recognition, the ACR. You can turn that off on many of the TVs we looked at.

CLAIRE GARTLAND: And for everybody's benefit, can you explain exactly what ACR is?

MARIA RERECICH: So ACR is a way to-- you can recognize what video is playing on the TV. Generally a fingerprint is taken of that data. It's sent out to third parties generally, sometimes the manufacturer. And they can tell what program you're watching.

Now a consumer hearing that often thinks that, well, OK, if I'm watching a network, if I'm watching a cable provider, that's the information that's going to be there. They already know I'm watching it, so if somebody else knows I'm watching it, OK, maybe that's not so bad.

But it's also if you happen to play a personal DVD that you have, and you play that. Any video content that's on the screen can be recognized, if it's something that matches up with what they're looking for. So you can see that.

So you can decide I don't really want somebody to know that, for whatever reason. Or you don't want it for the TV in your child's room or for anything like that. So you can decide to turn it off. Those controls are there.

However I haven't seen them called ACR off in the control. Not that anybody would know what ACR was in the first place. They're called different names.

The manufacturers have different buzzwords. One calls it Sync Plus. Plus sounds like it's good, right?

One calls it Live Plus. One calls it Smart Interactivity. Sounds very smart, sounds like something I want.

It doesn't say what it is. They don't have the information. Consumers should have the ability to know. It should be transparent what these things are.

And then they can decide it's OK, I'm all right giving that. I get value for that. I do get that value to have targeted content or second screen ability or any of these other things.

It can be valuable. We're not saying it's bad to give that data. But we're saying the consumers should know, the consumers have control over it and choice over it.

And another aspect of control and choice is deleting that data. When does that data go away? So some of the privacy policies we saw said that you can disable the service, and that data won't be collected anymore. It doesn't say what happened to the data that had already been collected under that service.

We found a really interesting-- I'll read you this-- a really interesting privacy policy I saw was set up in a very consumer friendly looking way. It was questions and answers. "How long will you keep my personal information?" So usually if you ask that kind of a question, you're thinking about I want you to not keep it forever.

But the answer is, "We will take reasonable steps to make sure that we keep your personal information for as long as is necessary for us to provide you with the service or for the purpose for which it was collected." So we will keep it for as long as it serves the purpose for which it was collected. That doesn't really say that they're going to delete it in a year or five years, or after you've thrown away the TV or sold it to somebody else or a million other reasons.

So we just think that things need to be clearer to the consumer. They can decide it's OK. I get a lot of value, if I give my data. I know what programming I get. I can get-- maybe I want advertisements that are targeted to me. Some people do, some people don't.

But you should choose. You should be able to choose. But you can't choose if you don't know.

MEGAN COX: And Serge, I think you've done some research on this too.

DR. SERGE EGELMAN: Yeah, I was actually thinking about this earlier, something that Ashwin said about if you ask people at Best Buy, do you want you know the benefits of personalization, you'll get a resounding yes, which is absolutely true. But if you ask the same person do you want your TV tracking you within your home, you're going to get a no.

And so the issue is framing matters. So when you present choices like this to people, you need to give them both the costs and the benefits and let them make a decision. And it needs to be transparent and also in a way that the average consumer is going to be able to understand it.

What's difficult about studying privacy is that there are a lot of-- privacy is a deeply personal thing. People have very different privacy preferences. And basically it comes down to how people evaluate their own utility functions, in terms of costs and benefits.

For some people, the cost here outweighs the benefit. And so they're going to disable the feature. Others understand the cost, but the benefit outweighs that cost. And so they're going to opt in. And I think it would be great if we could get to a situation where that's actually happening because we have better disclosures about what practices are occurring and what both the costs and benefits are of those practices.

MEGAN COX: And we got a question submitted here for you, Maria. So talking about how Consumer Reports is engaging in this effort to create a framework around certain privacy practices. Is that because it's based upon a known or an assumption that consumers will make purchase decisions based on privacy practices and be able to move the market? And how is that known?

MARIA RERECICH: Yeah, I think that if consumers know they can decide whether it's worth it to them to choose-- you know, if there's two equal TVs in our testing, but one of them gives a better privacy landscape or security landscape, data practices than the other, the consumer can decide whether it's important to them or not. And if the consumer decides it's important enough to them, it will move the market. Manufacturers will change what they do, if that's going to happen.

So we have a unique ability to be able to get that sort of information out. And it would be interesting. Now if consumers don't make a difference either way, then we know that too. But we think from everything-- the surveys that we've done, that Serge has done-- we think people do want to know, do care.

MEGAN COX: And Emmett, if I can come to you. I think that in the lead up to this workshop and in studying these issues and from everything we've heard today, it's known that there are certain controls in place. Whether they're well-labeled or accessible, that's an evolving landscape in early days here, with all these different types of devices and platforms.

Do you see self-regulatory efforts pushing for kind of a more unified opt out landscape and for controls for consumers? I think that we've seen convergence, like you said, in different app universes and on different devices. And so do you see that moving to the smart television space as well?

EMMETT O'KEEFE: Anything is possible. At least at DMA, we will certainly investigate things that our members and their customers want. I can't predict where that goes.

But just if I may step back again for a second. Here we're having an interesting conversation where, I think it was Justin's presentation earlier. They did some testing, and I forget the gentleman's name who helped with the testing or did the testing.

But they talked about how basically of the devices that they tested, almost all of them had notice and opt out of some form, what they thought were decent privacy controls. And so that's a good thing.

On the other side-- or not on the other side, but in parallel-- we've got the raging success of these devices and these online services. They're flying off the shelves. Manufacturers aren't making smart TVs just for their own benefits. They're making them because people-- there must be a demand for it. I don't mean to speak for anyone in that space. But it wouldn't be the case that they're making them, if people didn't want that technology to exist.

And so we've got people wanting their TVs to be smarter. My sense is that they're excited to have this functionality built into their devices. They have the opportunity to look at the user controls that are there.

We could have a separate conversation about how effective those controls are, meaning what words should be on the page and what shouldn't be. But I feel like we have a system that's working pretty well right now. But as far as our self-regulatory process, certainly we're happy to look into other control mechanisms, and whether there's consumer demand for more uniformity. But I can't predict it right now.

And then of course, there's always the countervailing concern that anytime you talk about a universal opt-out of some sort that you may end up collecting more data than less and create more privacy concerns, as an unintended consequence. But that goes without saying.

MEGAN COX: Well, we're moving to the end of our time now. So I wanted to go down the panel here and allow for each of our panelists to share their closing thoughts on what the future holds in this area of smart entertainment and consumer privacy. So Serge, do you want to begin?

DR. SERGE EGELMAN: I'm not really sure what I can add that wasn't already said. I mean, the conclusion is I think we need better disclosures, in terms of what the practices are, so that people can make more informed choices. Where the trade-off is between regulation and self-regulation, it's not quite clear. But as it stands, I don't think that there's a strong track record for self-regulation in this area.

So another example is AdChoices. So you know, that icon that appears in ads, people can click this icon to opt out of tracking. And the studies that have been done on this have found that one, most people don't notice the icon.

So this has been standardized. There is a standardized icon, which isn't the same thing as comprehensible or noticeable. So people don't notice it. And those that do notice it, have no idea what it means or what their choices actually are.

So I think that it's great, if industry wants to push for standardization, and I think they should. But I think effort needs to be put into making sure that whatever is standardized is actually benefiting consumers, in terms of being noticed, giving them choices, and helping them understand the actual practices.

MEGAN COX: Thank you, Emmett.

EMMETT O'KEEFE: I'll speak up for the Digital Advertising Alliance. DMA one of the founders of the Digital Advertising Alliance. And we take a very different view. I mean, it's out there in 90% of the-- I guess there's 90% participation rate in the DAA. It does afford notice and choice. Anyone who wants to click on that and opt out, they're certainly welcome to do that.

But how consumers react to it, yeah, there can always be more education. But the service is out there. It's functioning. People have choices, they have notice. We see that as a program that's working rather than not.

My overall message is I'm glad we're here. I thank you, again, for having this conversation. I am still struck by the notion that all the metrics say that we're in this golden age of television. There's more content that's out there that's at people's fingertips in a new way, that has never been there in any way, shape, or form in the same way before. It's working.

So our overall goal should be a, let's keep it going. And if we need to have conversations about things around the edges, let's do that. And we think that if other issues arise, it could be handled through self-regulation.

MEGAN COX: Thank you, Dallas.

DALLAS HARRIS: So I just wanted to first thank you guys, the FTC, for having me here and for holding this important panel. The recent election has put me out of the prediction business.

[LAUGHTER]

So I'm not going to make any guesses as to what the future may hold. But one thing I do know is that agencies like Epic and Public Knowledge will continue to be monitoring this issue as new technologies evolve, as smart TVs get connected with your smart refrigerator, and as these things continue to happen, to ensure that consumers remain protected. So I know we're not going anywhere. And we look forward to the innovation of the future.

CLAIRE GARTLAND: Thank you. So this panel has really talked about a lot of issues that can apply across the board. We've talked about how the same issues with disclosure and user control are just as true when we are talking about websites or apps on a mobile phone or a smart TV.

But something that is really unique about the smart TV conversation is that Congress, which doesn't legislate that often on privacy, passed not one but two laws protecting the privacy of what you watch on TV. So there's the VPPA, and there's the Cable Subscriber Privacy Rules. So this really reflects an understanding from Congress and a consensus that we agree that what we

watch in the privacy of our own homes should be private. The Supreme Court has also recognized and given the higher privacy protections for what happens in the privacy of your own home, in a family's living room, on their TV. These are private things.

And I think in terms of my prediction for the future that people will continue to want these protections to be respected. And they will continue to value the privacy of what happens in their home, when they're watching TV. And I think that in order to continue to facilitate consumer trust in not only the device manufacturers but the providers of all of these excellent services--which I agree are great.

We are definitely in the golden age of TV. But consumer trust is delicate. And I think that the industry players in this space will have to start to recognize that people care about their privacy and respect that.

MARIA RERECICH: I think Emmett's right that consumers really want these TVs. There is a lot of TVs being made, they're being sold, they're flying off the shelves. And it's great technology, they're great TVs. Advances are being made, pictures are wonderful, everything's really nice about these TVs.

These new features people do want. It's just that do they really understand what they're getting? It's only a question of let them make the decision whether the value of the data that they're giving is worth the benefit that they get. They deserve to be able to make that choice for themselves.

I don't think it's a negative thing. I don't want it to sound like it's negative, and we shouldn't have consumers giving data. It's that they should be able to know. That's all. And that's really I think the main part from my standpoint about what we're looking for.

MEGAN COX: Well thank you, and thank you all. Please join me in giving a round of applause for our panelists.

[APPLAUSE]

Thank you all for giving such careful, thoughtful consideration to these issues. And thank you all for joining us here today. This webcast will be posted on our website, alongside the slides that you saw here today.

We ask you to please turn in your name tags as you exit the building. We reuse these lanyards. We will be collecting comments until January 6, so if you have other thoughts to share with us today or in response to things you heard today, please do submit them. And PrivacyCon is coming up on January 12, so we hope that you will join us for that. Thank you.