FTC PrivacyCon
January 14, 2016
Segment 1
Transcript

[MUSIC PLAYING]

CHRISTINA YOUNG: Excuse me everyone. Can you take your seats please? I think we're starting.

Good morning and welcome to PrivacyCon. I'm Christina Young, a paralegal in FTC's Office of Technology Research, and Investigation, or OTEC. Before we commence I have some brief housekeeping details run through with you. First, if you could please silence any mobile phones and other electronic devices. Second, if you leave the building during the event you will have to come back through security. Please bear this in mind, especially if you're participating on a panel so you don't miss it. Most of you receiv

PrivacyCon with remarks from FTC Chairwoman Edith Ramirez who has led the agency's efforts to protect consumers from unfair and deceptive privacy and data security practices. Chairwoman Ramirez.

EDITH RAMIREZ: Thank you, Dan. I'm delighted to be here with you. So good morning everybody, and welcome to PrivacyCon, a first of its kind conference at the Federal Trade

Most recently we held a workshop on cross device tracking. To evaluate the benefits and risks of cross device tracking we need to know what it is and how it works. Our workshop included a session where experts explained how tracking techniques function and discussed whether technical measures such as hashing might be used to protect consumers' privacy.

And just last week we issued our big data report which outlined a number of suggestions for businesses to help ensure that they're use of big data analytics produces benefits for consumers, while avoiding outcomes it may be exclusionary or discriminatory. In this report we highlight possible risks that could result from inaccuracies or biases about certain groups in data sets, including the risk that certain consumers, especially low income or under served consumers, might mistakenly be denied opportunities where the big data analytics might reinforce existing socioeconomic disparities.

On the enforcement front, the work to tech researchers has helped us identify deceptive or unfair practices of companies such as HTC, Snapchat, and Fandango. Last month we announced an action against Oracle in which we alleged that the company's failure to disclose that older insecure versions of Java would not be removed as part of the software update process. We alleged that that was a deceptive practice.

Various researchers had pointed out problems with malware exploits for older versions of Java which led to our investigation of the issue. The consent order that we entered into requires Oracle to make an effective tool for uninstalling older versions of Java available to consumers. In short our enforcement actions have provided important protections for consumers and researchers have often played a critical role in helping us achieve that goal.

In certain areas we've also asked technologists and researchers to help us come up with technological counter measures to address vexing problems. Illegal robocalls are a key example. Voice over IP technology allows callers to spoof identifying information such as the calling parties phone number. Fraudsters can now place millions of cheap automated calls for with the click of a mouse. And they can do so from anywhere in the world that has an internet connection, while hiding their identities in the process. These developments have reduced the effectiveness of the FTC's traditional law enforcement tools.

Recognizing the need to develop new solutions the FTC has held four public contests to spur the creation of technological solutions to the robocall problem. As part of these robocall challenges we solicited technical experts to help select the most innovative submissions. One of the winning solutions in our first challenge Nomorobo is in the marketplace and available to consumers. Nomorobo reports that it has more than 360,000 subscribers and that it has blocked more than 60 million robocalls.

Given the importance of research and technical expertise in so much of the FTC's work we're also continuing to build our internal capacity. Last year we created the Office of Technology Research and Investigation or OTEC as we call it. OTEC, which builds on the work of our technologies and developments in the marketplace. With OTEC we're embarking on an even broader array of investigative research on technology related issues that will aid us in all facets of the FTC's dual consumer protection and competition mission.

[APPLAUSE]

JUSTIN BROOKMAN: Good morning everyone. Thank you very much Chairwoman Ramirez. Thank you all for coming out to our first PrivacyCon. I am Justin Brookman. I'm Policy Director of the Office of Technology Research and Investigation. We are co-presenting this workshop along with the Division of Privacy and Identity Protection. And I'm also the chair of our first panel, the current state of online privacy. If my co panelists could make their way to the stage.

So we put out our call for research proposals. We weren't really sure what to expect and we got nearly 90 really fascinating proposals. So originally we're going to try to do 12 or so. We decided to pack the schedule to have at least 19 people presenting and wish we could have done more. So we try to maximize the schedule to let them present their research to you.

They're each going to present for about 15 minutes. We're going to try to keep them aggressively to that. They have a clock right there that shows when they're over time. They'll be a chime in

In conclusion the Web Privacy Census is a modest research project that seeks to introduce reliable empirical data on the issue of how much tracking there is on the web. We have found provider--

Probably the most well used prior to us building our infrastructure. And we took all the features that had, added some more to it, and built it right into our platform as well.

So we give a researcher access to these different locations in the browser and then we wrapped that up in something called a browser instance. And as you can see here we're basically able to run multiple instances of Firefox, or multiple browser instances, at the same time. So when we do our own crawls. We run it over say 20 browsers, and each one has their own instrumentation. So you can easily scale this up to do measurement on a lot of sites.

And there's a couple things this lets us do. We can keep a profile consistent through crashes or freezes so we can keep the same cookies as we browse the different sites just like a real user would. We can also do things like run this with extensions or privacy features. See how well they work. See if they're actually protecting users or where they're falling short. And if there's any

were always more correct than the other groups about existing law and business practices. And not only that people who shopped online where less knowledgeable of rules and practices than people who didn't shop online. Strange. Right? You'd think those people shopping online would read a privacy policy.

started to do this in security. If your privacy policy says anything about security it requires some type of reasonable control over our personal information.

Another approach comes from the history of the Federal Trade Commission. In the 1970s the Federal Trade Commission started recruiting marketing academics to come in house support BCP and this greatly punched up the Federal Trade Commission's understanding of how consumers were misled by false advertising. And if you look at today's commission actions their false advertising theories are much more in line with how consumers really understands adds and how consumers really act. And that has not come over to the privacy side. So we could replicate that.

And then finally I do think that we need to look at unfairness more as a remedy for privacy problems. Now why is this? Notice and choice might work in a world where you're selling

Bain & Company, reflecting that. At the same time observers agree that people often release data about themselves that suggest much less concerned about that. Okay? That's called among many people, the privacy paradox. The notion that people say they love privacy but in everyday life it's program. Ad choices, those little icons that you're supposed to see. I gave a talk at the Penn law school one day showing a slide and nobody saw it. But they could point to this. And to sound more optimistic about what the public is than people like me or policymakers about this.

So we did a survey to try to look at some hypotheses related to this. A 20 minute, on average, interview taking place in February and March 2015. English speaking or Spanish speaking. 750 land line. Wireless 756. Conducted by Princeton Survey Research Associates. More data about that is in the paper. We look first at people's philosophy of trade offs. Not the particulars but what do they know about, what do they think about the idea of a trade off. And you can see it says, "If companies give me a discount it's a fair exchange for them to collect information about me without my knowing it." 91% said no. It's fair for a physical store to monitor what I'm doing online when I'm there in exchange for letting me use the store's wireless internet and Wi-Fi without choice. 71% said no. It's okay if the store where I shop uses information it has about me to create a picture of me that improves the services they provide about me. 55% said no.

Now oddly if we look at how many people agree with all three propositions, only 4% agreed with all three propositions. We took a broader idea of what agreement was when we gave you numbers to each, like agree strongly, agree, disagree, disagree strongly. And in that broader interpretation of

43% to around 20% is inconsistent with marketers' assertions that people are giving up their personal information because of cost benefit analysis. In the supermarket scenario, they're doing just the opposite. Resisting idea of getting data for discounts based on some kind of analysis.

Then we went ahead, our hypothesis about resignation came out of every day realization, when we met people, they would say things like, gee, you know, I have to give up the data. I want to be online, I have to be on Facebook. I know they do this stuff. I don't know. I don't know what's going on. But I have to do it anyway.

So we gave the people two statement separated by many other statements so they weren't right next to each other. I want to have control over what marketers can learn about me. I've come to accept that I have little control over what marketers can learn about me. Okay? It turns out that 58% of people agree with both things, which we say indicates a sense of resignation. Resignation, meaning the acceptance of something undesirable but inevitable. Got that from Google dictionary.

We've found there is a strong positive statistical relationship between believing in trade offs and accepting or rejecting various kinds of supermarket's use of discounts. You'd expect that. By contrast, there's no statistical relationship between being resigned to marketers use of data and accepting or rejecting the supermarket trade off. People who are resigned, sometime they do, sometime they don't. They're trying to navigate a world that they don't understand, are annoyed about possibly, and they sometimes will do it. They may look like they're accepting trade offs, but in their head they're saying, gee, I'm resigned to it.

Put another way people who believe in trade offs give up their data predictably, while people who resigned don't do it in a predictable manner. They do give up their data though. We found 57% of those who took the supermarket deal were resigned. A much smaller 32% were trade off supporters, even using the broader measure of trade off support that I suggested. The larger percentage of people in the population who are resigned compared to those who believe in trade have more knowledge than others. So having more knowledge is not protective, as some academics have suggested.

So what do we do about it. The rationale of trade offs is a fig leaf we argue, used by marketers to justify a world of tracking and increasingly personalized profiling that people know is there, don't understand, and say they don't want. We haven't begun to consider the social implications of having a large population that is a resigned about a key aspect of it every day environment. Now this may sound really dark and what do you do about it. But I think it's really important to confront what I see in everyday life when I talk to people. That people do these things online in stores with apps, not because they're thinking in a cost benefit way rationally. But because they feel that they have no other choice if they want to live in this world.

We're only at the beginning of key aspects of this era. This is the beginning of the new era, not even in the middle. And there may be time for concerned parties to guide it. Academics, journalists, and advocates have to translate the key issues for the public. And there are a lot of issues of obfuscation and deception we could talk about. Issues at the FCC might be involved in around public interest, convenience, and necessity. The importance that people alluded to, to praising and naming groups that do the right things and not to right things. Thanks for listening.

[APPLAUSE]

JUSTIN BROOKMAN: Thank you Joe. Thanks to all of our presenters. And now we're going to move into a brief period of discussion, with one caveat. Joe may have to leave early. He's teaching two classes later today at Penn. So if you see him slink off he's not in trouble, we're not angry with him, he's not mad at us,

So I'm going to start with some of the trends I saw some of the presentations. One is the proliferation and growing sophistication and growing complexity of online tracking was reflected in Ibrahim's and Steven's work. There's more cookies. There's more companies who are doing it. I love the revised lumiscape chart with all the hundreds and thousands of companies that can even see them on the big screen. And more technologies too. It's not just cookies, it's HTML5, it's fingerprinting, it's e-tags, it audio beacons, it's who knows? And then logically, perhaps unsurprisingly, then the theory of Joe and Chris's argument is that there's an increasing inability of consumers to really manage or control their privacy. Given all these advances.

So the idea that a consumer goes to a website and reviews the privacy policy, and makes informed choice and I am satisfied with how e-tags are used on the site, and I will now access my content in exchange for that is perhaps flawed. And this builds somewhat on Laurie Cranor's have tried to walk through deleting cookies or installing AdBlock, but he had to go pick up his what standards infer. It may also create a situation where sensationalist media stories or small vocal subsets who resist certain practices, end up controlling the conversation and give a false sense of clear consensus. And the last point would be, does this that entail a system where we must wait for harms and abuses to occur before we can then create systems to correct them, and if so, does that imply that along with some transparency mechanics, we also need mechanisms that consumers can see for due process and redress.

OMER TENE: Thank you. So I think all four presentations here drew sort of grim and somber picture of the state of play today with consumers being misled or resigned, and kind of being dragged along for the ride by technology or by business. Given that the stars seemed aligned on this. I feel an urge to play devil's advocate. And in that role I'm going to suggest a couple of different adjectives to describe how consumers are acting, or feeling, or faring. Instead of being resigned I'll suggest that actually thrilled, or maybe even exhilarated or delirious about these new technologies. About the fact that they can hail an Uber and rate the driver. And get the newest iPhone or Android phone and even, yippee, take a selfie, and post it under a SnapChat story. Or use a FitBit and give up their fitness or health information.

And I think we clearly see that in the marketplace. We also see Google and Facebook and Apple, Microsoft, three or four of the strongest brands in terms of brand recognition in the market. And not to mention the number of people flocking to work at these places including people who are now in government and even in regulatory agencies. So the point is that there seems to be something more complex at play here. And you know, I think we see it in another contexts. So I care about health, but I still eat a cheeseburger. I care about the environment, but you know, I drive a four wheel drive. There's a lot of snow in New England. And I think part of your response, your retort, will be yes, but consumers are ignorant. They just don't know. But actually I think Joe's survey and research shows that the more informed, they become more resigned. So maybe it's better to just be blissfully ignorant. So with all that I want to turn back to you and hear your reaction.

JUSTIN BROOKMAN: Do you want to start?

JOSEPH TUROW: I mean these are really important insights. I think that it's a complicated world. It's very hard not to be excited about the ability to walk through a store and compare prices in your hand. There are levels of excitement about being able to show a kid a snippet from the Wizard of Oz on a phone, on a understand the political process when they think they're getting information that is developed personally for them, that are personal ads. And so while I agree that there are many terrific things about this. I think that there have to be segments of society, they have to say, stop, we can fix the really difficult things that relate.

CHRIS JAY HOOFNAGLE: Let me unravel some of the issues. What I'd say is that at first but one can look at our work and say it's anti-technology. But I would argue strongly that it is not. I personally love technology and I'm an early adopter of many, many things. I'm also a practitioner. And I do know that much what we call innovation does not depend on personal information. And is fundamentally compatible with what Alan Westin would call modern information privacy law, such as, we're going to de-identify this information after six months. We're going to delete it after a year, et cetera.

So I think one of the rhetorical, it's in a way straw man, that we have to recognize and deal with, is the idea that we can't have privacy and these technologies. We can have Uber. Uber is actually not that innovative. Long before Uber taxicab companies had hail apps and blah blah blah. Don't need personal information for a lot of that. But where you do need personal information you can have rules around it. And I see it from practice all the time. There are situations where we do very interesting forms a personalisation with de-identified data, where we agree that data will disappear after a certain amount of time. Where we agree that certain things won't be the basis of selection and the like. So I think we shouldn't fall under the false dilemma that privacy means we cannot have spectacular convenience in our life.

STEVE ENGELHARDT: So coming at this from I guess from the tracking perspective I wanted to comment on the fear of maybe users becoming resigned by getting more information about what tracking was going on, or the notion that we can't have the services without having the tracking. Because I think there is definitely a cha(i)-2()-6(et6(h)-4(a)]TJ   o)-4(f)-1(i)-6(ever)-1(e)d5(i)-6(t(w)9 like the FTC or the government could be making prescriptive, paternalistic choices on behalf people. That has its problems as well.

One thread we've heard a few times today is the idea of increased transparency, and then filtered through elites or institutions. And then the name and shame approach that Joe and Steven talked about and Elana talked about in her comments. I guess my question is, is that scalable right? I mean The Wall Street Journal did their "What They Know" series starting in 2010. And yet the reports you guys show is that the tracking that they're concerned about is still increasing. Joe and Kristin have been doing this for even longer. So what is the policy solution? Assuming that this is a problem to be addressed. What is the right approach?

OMER TENE: Can I jump in and say that?

JUSTIN BROOKMAN: Yes.

OMER TENE: Thank you. That I think. And also reacting to what Chris and Joe said, I think there is consensus that we need to deal with data excess, and have the identification and strong data security. But I think to a large extent the industry gets it and certainly industry gets the big impact that privacy fails can have on brand and consumer expectations. And I think one thing that attests to this is the fact that we're having this conference and the existence of a privacy profession that has blossomed so the IPP now has a 25,000 members worldwide, that had less than 10,000 just two and a half years ago. I think the right processes are in place and it's really the excess that we need to deal with. And I think you illustrated this some of this in technological research.