FTC Informational Injury Workshop
December 12, 2017
Segment 2: Panel 1
Transcript

DANIEL WOOD: To start off today's workshop, we'll be exploring the broad array of negative outcomes that result from unauthorized access or misuse of consumers' personal information. We're fortunate to have a panel of experts today who can speak to a wide and varied range of injuries. We hope that this first conversation will provide concrete examples that later panelists can draw from while discussing various aspects of informational injury.

So we have five wonderful panelists that we're very happy could join us. And we'll spend the majority of the panel hearing from them. We're planning to devote the last 10 minutes to audience questions. So if you'd like to ask a question, you need to find a question card. They are outside the auditorium. Or you can also raise your hand, and I believe paralegals have them. Then, you pass the question card to a paralegal, and they'll bring it up here.

So with that, let me introduce the panelists. So Pamela Dixon is the Founder and Executive Director of the World Privacy Forum, a public interest research group known and respected for its consumer and data privacy research. Damon McCoy is an Assistant Professor in the Computer Science Department at NYU Tandon School of Engineering. His research interests are in the area of security, privacy, and empirical measurement. Some of his current interests span from the socioeconomics of cybercrime to automotive computer systems.

Lauren Smith is Policy Counsel at the Future of Privacy Forum where she focuses on big data and the Internet of Things as related to connected cars, data ethics, algorithmic decision-making, and drones. Cindy Southworth is the Executive Vice President of the National Network to End Domestic Violence. She founded the Safety Net Project which focuses on the intersection of technology and intimate partner abuse.

Finally, Heather Wydra is Supervising Attorney at Whitman-Walker Health's Legal Services Program. Her practice areas include discrimination in employment, by places of public accommodation, and in health care, as well as representing clients who have been denied access to health insurance coverage or disability benefits. Now that we have those quick introductions done, let's get this panel and the workshop itself started by discussing the various types of informational injuries and consumer harm that our panelists have seen.

JACQUELINE CONNOR: Thanks, Dan. My name is Jacqueline Connor, and I'm an attorney with the Division of Privacy and Identity Protection. And so today, we're going to start the panel off by asking each panelist one question and giving them some time to answer it. And then, we're going to jump into a more general group discussion where I hope that the panelists can jump in whenever they want to. So Pam, we're going to start off with you, and I think you have the clicker there for the slides.

PAMELA DIXON: Thank you.

JACQUELINE CONNOR: So unfortunately today, I didn't [INAUDIBLE] as the term has become part of our everyday lexicon. And the harm posed to consumers goes beyond what we consider quote, unquote "traditional" identity theft. Can you describe some of those other different types of identity theft?

PAMELA DIXON: Sure. First, thank you for the invitation to share my research and knowledge here today. And I'm really grateful that the FTC is holding this workshop. I think it's good timing and a good topic. So thank you. So I think everyone is familiar with various financial forms of identity theft. We have probably all experienced an incident where we get a phone call from our financial services company, and they say, by the way, we're going to issue you a new card because someone's using your card.

So that annoyance is a lot different than, for example, the woman I met and worked with who was from Utah who had her children taken away from her through the actions of a medical identity thief. In her particular situation, what happened is that an impostor had taken her identity information, just gleaned from a simple phone book call. And this woman went around to emergency rooms around Utah seeking painkiller drugs. And the police came and when they arrested this person who was a problem, they came to the victim's house, arrested her and took her kids away from her because she was a bad mom for being a drug seeking behavior person.

So it took her three months and a DNA test and working directly with the state attorney general to get cleared and to get her kids back. So medical identity theft poses extraordinary harms to its victims. And Acting Chairman Olhausen discussed quantifiable risks. We released a report today called "The Geography of Medical Identity Theft" where we worked very hard to quantify the patterns and distribution of medical forms of identity theft.

When medical identity theft happens, it usually happens by the actions of organized crime or very organized professionals who are working within medical and billing systems to create false billing situations. Sometimes, it's the action of rogue individuals, like the woman who had a problem in Utah. But no matter how it happens, people who have had their identity used by others to procure or bill for medical goods and services that they themselves did not seek nor receive, have unique harms.

The first core harm that they have is that fictitious entries are entered into their medical file. Typically, it's a very expensive disease, for example, HIV/AIDS, sometimes cancer treatments. A popular thing to add to victims' files is Hepatitis C treatment because it can run up to about $1,000 a pill, leading up to about $120,000 that people committing the crime can pocket for

And what is happening is that this crime is victimizing certain states, certain genders, certain ages, the very young, the very old. And what's happening is that you're seeing real pockets of quantifiable harm. So let me move to the slides very, very quickly, and let's see if this works. It's going to work. So we did a very substantive statistical analysis and culling through just loads and loads of complaints to the Consumer Financial Protection Bureau.

Now, these particular complaints are just the simple count of report. So in other words, these are the pure counts. If you look at this diagram, you can see California because they're a populous state. They've got a huge roster of counts, same with Texas, and same with Florida. You can see

Well, subject two comes along. And he's like, you know what, I would really like some free health care, or I would at least like to do some fake billing so I can sell some things on the street. This hospital has a biometric enrollment system. Let me go ahead and take his driver's license scan that the hospital so helpfully has stored for me. And let me use free technology to morph my photo with his. And we'll create that middle image that you see, morph one plus two.

Well, unfortunately, it is very unambiguous research at this point that subject one, with the original photo, and subject two, with his original photo,-- based on that center morphed photo, both of those subjects will be authenticated within that health care system. So what we're seeing on the street now is clinics and other bad actors taking biometrically morphed authentications

And these doxes normally include the names of the people, their online aliases, their age, their date of birth, their addresses, phone numbers, sometimes medical information about them, ISP information, and also a lot of information on the family of these victims. And it also includes things like their online social networking profiles, and things like this. And so these doxes are oftentimes posted with the hope that they are trying to encourage harassment of the victims of these doxes.

And so in one of my studies, we actually built a system based on some machine learning that was able to go out and find about 6,000 of these doxes. So we ran the system for about 12 weeks, and we found 6,000 of these doxes. And probably the ones that we found were only the most egregious of these doxes since our system was fairly conservative about what it called a dox. And so based on this, we could do some analysis of these doxes.

And what we find is that the victims often come from one of two communities. They either come from the gaming community of video gamers, or they come from the community of hackers and underground actors. And the other thing we can see from this is that the victims oftentimes skew very young. And so the victims are oftentimes in their teens, perhaps in their early 20s.

And so this is very targeted and impacting, not the people likely in this room but the younger generation of people. And as you can see from the 6,000 doxes that we found, and this was not a comprehensive study, that this is happening very frequently and impacting a lot of people's lives. And so one of the, probably, most egregious harms that can happen from this is in those doxes, again, they include people's social networking profiles. And, again, this is done to encourage other people to pile on and harass these people.

And so what you're looking at here is-- we actually did our study in two parts. So we did our study in two, six week parts. We found about the same number of doxes in each part of our study. And with these social networking handles, we pulled these out of the doxes automatically. And we monitored the privacy settings of these people's accounts. And what you can see from this graph here on that first one is that red part is essentially people closing their accounts down.

So this represents people becoming socially isolated, likely being forced by harassment to close their Facebook accounts because of these doxes. And so what you can see in that first period is that the thickness of this is the magnitude of the number of accounts that are closing it down. And so that first part is before Facebook started deploying filtering to try and filter out harassing comments from their platform. And that second part is after Facebook deployed filters to filter out harassing comments from these.

And you can see the huge benefit that was incurred by their population when Facebook did this. And this is actually a nice thing that we can show that this kind of harm can perhaps be mitigated by these filters that these online social networking sites are deploying. The other kinds of harm, probably the much more dangerous kinds of harms, that can come from these is, again, the phone numbers and addresses are also included in these doxes.

And so this can lead from fairly innocuous things, like someone ordering a pizza to someone's house, to someone creating a fake emergency situation, say like, they make up a situation where

it's a hostage situation or something like that. And they call up 911, and they say there's a

And then, there's stuff that's off of these stores that's much more egregious. And so a lot of these developers, as you can see from this marketing material that I have posted up

So in a lot of instances, analysis of sensitive data categories, such as race, gender, or pregnancy

And for the first under individual harms, we drew a distinction between those that are unfair and those that are illegal because we felt that there is more clarity in, especially, civil rights law as well as FCRA and some other areas where specific harms to an individual have already been identified as illegal as there is clear societal consensus that we do not want these harms to occur and can use technology to ferret out and to prevent some of those harms.

And then, the ones that are not as explicitly illegal can raise questions of unfairness and of ethics but may require us to do a little more thinking to determine in what instances this would be considered an injury to consumers, and how one might want to think about identifying and mitigating and being aware of some of those concerns that might arise with automated decision-making overall.

So when we got to the substantive grouping of the harms, we found that by and large they could be grouped into four broad buckets. So the buckets are loss of opportunity, economic loss, social detriment, and loss of liberty. And we thought that these depicted the spheres of life where

You have job loss that you can have if you are identified as a victim. Unfortunately, there's still a huge stigma. Some people will say it's not safe for you to work here. You might be a risk to your colleagues. So you see all sorts of discrimination type things that Heather's going to be touching on more. And other things to think about is just how data in combination can be problematic.

And so years ago, AOL released some of their search data for research purposes and didn't realize how identifying it was. A reporter actually took that data set, realized that somebody was searching for themselves by name and also searching for things like domestic violence, shelter, protection orders. So the reporter called the victim up and said, hey, I got your information from

was transgender. I worked recently with a client who was going to her gym, having absolutely no problem. She was a transgender female.

So just to give you your trans 101 training, that means she was identified as male at birth but had been living outwardly as female for years. But she hadn't changed her driver's license. So she was going to the gym, using the women's locker room. Everything was fine. But then one day, she didn't have her ID card and had to show her driver's license, which was old. It had an old picture and an old name.

And then after that, everything changed. The manager said she couldn't use the women's locker room anymore. So we're currently dealing with that case. As some of you may know, in DC the law is very clear. It doesn't matter whether identity documents are formally changed or not. If somebody identifies as male or female, that is the gender where they need to be treated under the law.

And so finally, I'll talk about the harm that can come in personal relationships when personal information is disclosed. There was an incident that happened with Aetna. It was in the news. It was public. Aetna sent a mailing to dozens of its HIV positive clientele who were-- they were making some change to how they were covering HIV medications.

And the mailing that went out had a very large window that shows the address where you can see what the address is. And the window was so big that it actually showed the first couple of sentences of the letter, which talked about HIV and medication. Well, these letters went to people at their homes. They went to people at their apartment complexes where mail is just thrown everywhere by the front door. And a lot of people ended up with their personal health information disclosed to family members, neighbors, friends, when they really didn't want it to.

Sometimes, that was OK. But we heard horrible stories, people who came to us wondering what they could do because, again, it ran the gamut from, people just look at me weird now to somebody wrote bad words across my apartment door and vandalized my garden and left me a note saying, we don't want your kind here. So those are the types of things that can happen to people when their personal information is disclosed without their permission.

DANIEL WOOD: Well, thank you very much, Heather. And thank you to all the panelists for describing to us a very wide range of injuries. I hesitate to ask, but are there other types of informational injuries that we haven't touched on yet?

PAMELA DIXON: Well, if no one is going to respond, I will. There are certainly more types of informational injuries, and they are hiding in every corner of the digital ecosystem. I think, though, that the important thing is to focus on what causes substantive harm and harm that has meaningful impacts on a person's life. We can all spend time working on issues, but there are big issues. I do think that medical forms of identity theft, I think biometric harms, I think these are big issues.

I think the issues we've heard around this table are big issues. If someone is going to have their life threatened or their livelihood threatened, these are profound harms. So in some ways, I

would really rather look at quality and say, look, here are very meaningful harms that we have quantified, we've studied, we know about. Well, let's roll up our sleeves, and let's do something about them.

We've had plenty of time to identify these harms. Why not have the FTC write a new report, for example, about domestic violence, about medical identity theft, about these other harms, hold a separate workshop. Let's find solutions. Let's work collaboratively. I'm all for instead of breadth, let's go depth. And let's solve the problems.

LAUREN SMITH: I'd say one area of harms that we haven't provided examples on yet appear as the loss of liberty harms that can have a very significant impact on folks' lives. So there's been a lot of good research on predictive policing and the fact that relying on data to determine how policing resources are targeted, if it's not done with an understanding of the risks, can reproduce historical bias and have a very significant impact on communities at large.

And I think those are things we're just beginning to understand and figure out how to mitigate, and things like use of recidivism scores, making sure we're understanding the type of data that is going in, assessing whether that is the correct data, assessing whether that data has its own biases built into it when we're making decisions about folks' literal freedom.

CINDY SOUTHWORTH: Just on that note around what police data can do. Police data can do a lot of mitigation of harms in terms of helping identify where you've got either over-policing or under-policing, or institutional bias dilemmas. One of the other downsides of police data is inadvertently it can actually be identifying. So there was a 12-year-old rape victim that her identity was basically compromised by a very well-intentioned police department publishing their police data.

And they'd used the block to try to anonymize the data, but there was only one adolescent girl on that block. So even the attempts to anonymize the data, it wasn't anonymized. And so in that case, a pretty traumatic life experience then became amplified by the whole world finding out about it.

let's be able to use technology and have it not harm us, that's really the situation I want to see people get to.

JACQUELINE CONNOR: Thank you. So moving on a little bit. What are the costs of fixing these informational injuries that you've all been talking about, financial or otherwise? And I know Heather was speaking to this a bit about legal remedies. But what legal remedies are available to consumers to address these harms? And if there's not any, what gaps are there? And what are the consequences? I know that's a loaded question.

HEATHER WYDRA: Well, I can start talking about the clients that I work with and the cases that I see. The remedies, if they exirk0.002 Tw 0 -2whor ot (ex)-14 ()-6 (h/)2 (th)2 2 70 (I)2 thrk0. (i)-6 Yu02 Tv

tech platforms to define societal norms? And is that too much to ask as we're thinking about these issues?

And considering that for things like network bubbles and narrowing of choice, we haven't created a clear set of societal norms yet. But if there are business processes that are taking these into account, that are considering the ways in which these products could have impacts like this, creating ethical frameworks, creating best practices to monitor and check for ways in which data and a data set could be used to have some negative impacts, but that is really something that should be baked into how we're thinking about new technologies going forward.

DAMON MCCOY: So I think one big area that we've obviously seen a society that's lacking in laws is this online hard be onli o 0 TIueke thishidox10 (i-10 (g)1 (t)-2 (ha)4 (t)-2 ( )]TJ 0 -13 ( )-113(o 0 TI)w

And if people see their screens, they can quickly infer other things that people are searching, that are oftentimes very private.

PAMELA DIXON: I did think of something that actually I think is an everyday informational issue. Most people who call our office are interested in stepping up their privacy game. And one of the first things I ask them is how they're using their financial tools and services. And really, if you want to really see a lot of privacy informational issues that are on a lower level, not

DANIEL WOOD: Anyone else? Well, I guess we

But I think that that's been a part of everything we've all talked about. Of course, we want these types of data breaches and personal information to be protected but when it isn't, it has to be dealt with with compassion. And it's important to understand, as you just said, the types of harms that happen because it makes people more motivated to make sure that they don't happen.

LAUREN SMITH: And I would say, as we think about these injuries writ large, to ensure that we're approaching them methodically and really identifying the harms that we're most concerned about and separating that from what the causes might be and using that as a step to get to what the solutions might be, and then understanding that technology in its many forms today can create some of these harms but could also be used as a tool to prevent some of these harms that may have been perpetuated by humans and our less technological form before, but now could potentially be mitigated with these technologies.

DANIEL WOOD: Well, that's nice to end on a hopeful note. But we do have to end. So there will be a 30 minute break after this panel. And so the next panel begins at 11:15. The cafeteria is open until 11:00.

JACQUELINE CONNOR: It opens at 11:00, open until 11:00. Sorry.

DANIEL WOOD: Open until 11:00, then it closes. So if you want coffee, that is your best bet. And we'll see you back at 11:15.

JACQUELINE CONNOR: Thank you to our panelists.

DANIEL WOOD: Thank you very much to our panelists.