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 themselves. Meanwhile, the victim is left with Hepatitis C on their medical file, not a great thing to have there for all sorts of reasons.

So what on earth do these victims do to get cured? Well, unfortunately, there's not legal recourse to correct or delete medical information from files. Our geographic research that we published today shows that medical identity theft is, in fact, growing, but it's also doing something unique. It's growing in very specific regions of the US, for example, Florida and other areas where there are elderly residents that are clustered.

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 Georgia popping up there a little bit and New York. This is showing activity based on population.

But when you normalize the data and adjust it to count per one million, all of a sudden, the population density issue goes away, and what you get is this. So now, you have a different picture emerging. By the way, the report has 2017 data. What you see here is an absolute crisis. You see a very deep distribution of medical identity theft across the US. You can see, for example, Nevada, Colorado. Florida remains very high.

And actually, when you're able to look at the data closely, the entire southeastern chunk of the United States is a hotspot for medical identity theft crimes, and in particular, Florida. So here is a simple count of reports from 2016. This is, again, just a pure count. And I chose this to show you, just so you could get a feel for-- when people talk about medical identity theft, California has a lot of cases. You see a lot of DOJ activity in California because there are so many cases.

But then, if you normalize the data, that's what you get. And you get these profound patterns where serious harm is happening. People are having their health records falsified. In our research for this report, we found that people are literally unable to remove false billing records from debt collector scenarios. So these are profound harms. They're being targeted geographically.

And consumers and patients who live in these hot zones are going to experience greater risk than those, for example, who live in North Dakota. And it's not just based on population. It's based on targeting. So I want to quickly pivot to biometric identity theft. We're behind the eight ball in the realm of medical identity theft. It's in crisis proportions. And in biometric forms of identity theft, we will certainly wish that we would have dealt with it early. We still can.

And so that's why I'm very keen to present this to you. In biometric expert circles, there's something that's being talked about a lot. And we're, unfortunately, already seeing forms of this crime occurring. So what's happening is that health care providers are installing, and others, schools and financial institutions, and even federal agencies and other areas, are installing biometric measures to assure identity.

So it can be an iris scan. It can be a fingerprint, facial recognition, all sorts of things. But the way that biometrics work, it's math. It's not magic. And it can be spoofed, and it can be foiled. And this is one of the most difficult types of identity theft to prove your innocence of. So what you're seeing right now-- if you see subject one, let's just say that his identity information is stored in a hospital.

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 stringing a dozen people off of that authentication and passing people through.

So this is a risk that has not made it into the mainstream yet, but we're watching it very closely. So based on these things, I have just a couple of things I want to say in terms of harms and what to do. It is very clear that victims of medical identity theft, and advanced forms of identity theft like that, have experienced very different harms than victims of lesser forms of identity theft, such as credit card fraud. They are in a class by themselves.

And I call on the FTC to study and treat this form of identity theft as a completely distinct and separate class because there are completely distinct and separate classes of harms. And Congress definitely needs to pass specific legislation in terms of working to create remedies for these situations. It will require dedicated work from the FTC and other federal agencies, including CMS, working directly with state level AGs because of the patterning of medical identity theft.

For biometric harms, it's going to take a lot of money because these presentation attacks through biometric morphing, the only way you can fix it, really, is to have a secure line where you have a secure photo, not a Kinko's photo or a photo taken at an insta passport place or somewhere else. You have a secure photo that goes securely to whatever vendor is creating the final product. These systems are easy to spoof also in other ways.

So if someone is taken over your biometric identity, it's very hard to prove your innocence. These are distinct harms. We've got to study them, benchmark them, and work very diligently on their specific and unique harms. We can't lump identity theft as a category together anymore.

JACQUELINE CONNOR: Thank you, Pam. You can pass the clicker on to Damon. So Damon, as we just heard about medical and biometric identity theft, those might be new topics to some. But it's fair to say that most people know at least a little bit about identity theft. However, there are still abuses of personal information out there that people may not know about, but that they're incredibly damaging to people. Can you explain what some of those are?

DAMON MCCOY: Sure. I'm going to go through a little bit of the research that I've been doing on this, starting with what's called doxing. And so doxing is basically the public release of people's information that they probably wished to keep private. And so for those of you that haven't stared at lots of these doxes, these doxes are posted a surprising amount of times on the internet.

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 hostage situation going in this house. And this triggers a response by the police departments to send armored SWAT teams to someone's house with guns blazing on to someone's house. And so this has resulted in many very dangerous kinds of situations.

Unfortunately, this kind of harm is more difficult to try and measure. But this is something that I think that we should do a better job from police databases and things like that to measure this type of harm that's incurred by doxing. And so the other question is, where are they getting this information from? And so one thing that we can notice from these doxes is that a lot of times they have ISP information. And a lot of times there's also online cookbooks as to how to gain information to dox people.

And a lot of times these include a method where they essentially social engineer call support centers, especially ISP call support centers. So they can start with someone's IP address that they somehow gain, maybe by playing a video game with them, and they can spider out and start to get more information. And so this is another thing where we should investigate how they're getting this information and, perhaps, understand how to make it more difficult for them to acquire information as easily.

The other way that they acquire information is by sometimes social engineering their victims into installing malware. And it's a particular kind of malware that they normally have installed on the victim's machine. It's called a Remote Access Trojan, or RAT for short. And so there's, unfortunately, underground ecosystems, like 4chan and Pastebin, where the doxes are posted.

So there's other hacker forums where they basically trade or talk about how to acquire victims, which they called slaves, to infect with these Remote Access Trojans. And when a victim is infected with one of these Remote Access Trojans, this effectively gives the attacker complete access to that person's computer, including the camera, the microphone, all of the files on the system the attacker can rummage through.

And so oftentimes, what crops up from this is what we call sextortion where the attacker somehow steals some sensitive information from the victims and tries to extort them either for more images or perhaps for money and things like this. And so a high profile victim of this was Miss Teen USA. She was infected by one of these RATS, and she was caught up in one of these sextortion cases.

But there's hundreds and hundreds of these victims. So, in fact, we did a study where we enticed attackers to attack our own systems. And we had hundreds of attackers, unique attackers, that visited our systems, many of them from the US but from all over the world. And the first thing that most of the attackers did is they tried to access our camera when they attacked our systems.

And so the final thing that we've been looking at lately is spyware. I think, actually, spyware is a misnomer for this. I oftentimes call it stalkerware. And so these are mobile apps that can be installed on people's phone. Some of these are in the, say, the Play Store and Apple's App Store. And they have dual use features. So they can be used, for instance, to find someone's stolen phone. Or they can be used to, without the victim's consent, stalk them.

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 here, are essentially encouraging people to use it for this use case of stalking their partners. And so this can lead to a lot of different kinds of harms. Probably the worst of these harms is interpartner violence. So this can be used to facilitate intimate partner violence. It can also be used, again, to stalk people.

And so doing just quick internet searches, you can find tens, hundreds of these different apps that abusers are talking about installing on their victim's phones. And again, we can see paid advertising where the developers of these kinds of stalkerware apps are encouraging and facilitating this use of their apps. And so throughout all of these studies, I can show that oftentimes there are cyber harms that are hard to boil down to dollars.

They are physical threats, emotional harm, social isolation, that are very hard to boil down into dollars. And they affect, oftentimes, young people, so the newer generation. And they probably have a lifetime of impact against these people that are harmed by these kinds of cyber attacks.

And so with that, I would encourage more of these kinds of studies to understand the scale and the other kinds of harms that are occurring, and also the intermediaries that are facilitating these kind of harms. So with that, I will hand it off.

JACQUELINE CONNOR: Thank you, Damon. So Lauren, so far we've discussed injuries that occurred to particular consumers. But what kind of informational injuries are possible when many consumers' information is combined?

LAUREN SMITH: Well, thank you for having me here to speak today. I'm excited to participate in the panel. And yes, I'm going to take a little bit of a broader view, to take a step back and think about the fact that as the volume of consumer data grows, the number of decisions that were previously made by humans are now increasingly being made by algorithms. As the number of data sources have multiplied, so too have the types of data involved in these decisions and the number of entities that may process and analyze this data across many sectors.

So I'm going to be talking about potential harms that come not just from explicitly fraudulent activities or hostile approaches that we've heard from some of the other panelists today, but instead look at areas where the collection of the data initially may have been legitimate uses, may have been offered up by consumers in exchange for a service. And as you mentioned, this can create a number of downstream effects. So information can be combined.

So a consumer may provide some information in some context, but in what is sometimes called the mosaic effect, that information could be combined with other data sets and, perhaps, reveal information that they may not wish to have out there publicly. And also, there can be inferences based on data that consumers have shared, particularly with the advance of artificial intelligence, that there may be information that could be inferred about a person from data about themselves that they may not have explicitly shared.

So in a lot of instances, analysis of sensitive data categories, such as race, gender, or pregnancy status can be used to improve services, promote inclusion, advance research, and actually be used to mitigate human bias. But in other contexts, it can raise the specter of disparate impact on vulnerable communities. And as a number of folks have sat down to try to tackle this issue-- I know my initial work on this started when the White House did a report on big data, looking at the benefits and potential risks arising from big data.

And one of the biggest areas that was a surprise to the folks working on this project and in the building was the intersection of big data and civil rights, and the way in which this growth and automated decision-making could wind up impacting civil rights. And the FTC has also done a lot of good work and hosted a workshop on that topic explicitly. So as my organization sat down to try to tackle this issue, we found that conversations on the topic sometimes become mired in definitional challenges that can make progress toward solutions difficult.

So these analyses sometimes failed to separate harms from the causes and from solutions. Sometimes, we wind up conflating human biases that have shaped society for years with digital causes. And this can make it difficult for a Consumer Protection Agency, like the FTC, to determine what kind of injury they should be protecting consumers from and how to define that.

So identifying financial injury around fraud, breach, or security failures may be fairly well defined as we've seen in several FTC enforcement actions. But in other contexts, identifying the injury may be more complex. We can run into issues like this with things like differential pricing, which has given us things like senior and student discounts for years without creating what we might consider to be a financial injury, but can raise new concerns as consumer purchasing moves to the internet and pricing can shift based on a range of consumer attributes.

So we found that there aren't many easy ways to navigate these issues. But we think that more can be done to promote fairness and encourage responsible data use. So to facilitate these conversations, we endeavored on a project that launched today that I'll give you a brief preview of, and there are handouts also at the front.

We reviewed the leading books and articles on this topic and tried to distill the different harms that are identified in the literature into a set of buckets and into a chart so that we can think about them at a very high level, and try to understand what are the types of harms that could arise from automated decision-making based on consumer data, so that we can have them all in one place and determine whether some of them should be considered more of a risk, more important to address and focus on than others, and whether mitigation strategies might differ depending on which types of harms you're talking about.

So you can see a bit on this chart up on the screen. So the first distinction that we made in groups of harms was the types of algorithmic decision-making that could either turbocharge or make more opaque harms to individuals, which you'll see is the left 2/3 of the chart. And on the right is collective harms, which may be a little more difficult to pinpoint because they may not be specific harm to a particular person but may impact us at the group level, either as a society as a collective or specific groups.

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 automated decision-making could potentially cause the most harm. And any of these buckets, as I mentioned, the harm could be illegal. It could be not illegal. It could accrue wholly to the individual or to a group.

So an example of an individual harm could be me not being able to rent an apartment because of a decision made about me or something entirely to society, which could be something like filter bubbles that have become a topic of discussion, especially around the election, that many of us may believe have a harmful impact on society overall but have not been distilled as clearly, at least in existing law, and may not be something that can be tackled at that level at this point.

So for loss of opportunity harms, this group broadly describes harms that occur within domains of workplace, housing, social support systems, health care and education. Economic loss harms broadly includes harms that cause financial injury or discrimination in the marketplace for goods and services. Social detriment largely talks about harms to one's sense of self, self-worth, or community standing relative to others. And loss of liberty applies to harms that constrain one's physical freedom and autonomy.

So these are up on the screen. In our packet, we give particular examples of each of these. And I'm happy to run through those individually. We recognize that these categories that I just ran through aren't mutually exclusive. Economic loss can certainly lead to loss of opportunity. But in our attempts to survey the literature and boil these down, we found these to be the most ready categories.

And then in an accompanying project, we also used these categories to then try to bucket them, the harms, into different groups that could be approached with the same sets of mitigation strategies depending on the way they're characterized in this chart.

JACQUELINE CONNOR: Thank you, Lauren. Cindy, given your experience with domestic violence victims, what types of informational injuries do you see arising and how?

CINDY SOUTHWORTH: I just wanted to take a moment to go back to the HelloSpy slide that Damon provided because it gives me great pleasure to trash them at every chance I get. So please, soundly tweet at them. They are foul human beings. This is how they advertise an alleged family safety product. It's all about encouraging and facilitating stalking and domestic violence. So I last trashed them in 2014 at a Senate hearing, but I appreciate any opportunity to go after miscreants like this.

On a more serious note, just a little bit about domestic violence, stalking, and sexual violence. Many people think of them as these tiny societal issues, this fringe thing. And when you actually look at CDC, FBI numbers, Department of Justice research, one in four women will be physically assaulted by an intimate partner at some point in her lifetime. That doesn't count emotional abuse and control and lots of other unhealthy and controlling relationships.

One in six women will be stalked by a partner or stalked. And one in 19 men will be stalked in their lifetime. And then, one in three girls will be sexually abused before they're 18, and one in six boys. These are staggering numbers. That means your CEO, your boss, your neighbor, your friend, your postal worker, your barista at the Starbucks, your next politician is a survivor of one of these crimes.

And so when you think about this large swath of society who's experienced significant victimization, then you think about how they're part of our daily lives. They're part of our data sets. They're part of our medical records. They're part of our lives. And so the Safety Net Technology Project that I founded 17 years ago, on our blog, techsafety.org, we did a survey back in 2014, and we found that the local domestic violence organizations-- there's about 2,000 of them nationwide that take those hotline calls from victims who are experiencing pretty horrific things.

And back in 2014, 97% of those frontline victim service organizations said they were seeing cases where tech was being misused by offenders and abusers, of course, because tech's part of all of our lives. We all have our hands right next to a phone. And three years ago in that same survey, we found that 71%, almost 3/4, of those local programs said that abusers and stalkers had started using technology to monitor internet and computer use, so essentially, spyware.

We don't have prevalence or incidence stats. This is just what the victim advocates are seeing on the ground, and the numbers are really quite concerning. When you think about some of the specific harms, the obvious one is illustrated above. It's the physical harm. People running for their lives still happens. Domestic violence shelters end up housing or supporting 72,000 adults and victims in a given 24 hour period. But 41,000 adults and kids are kept safe in a shelter or a transitional housing program on a given day, 41,000 people.

So they have significant privacy needs, and they are obviously quite concerned about data privacy and data security. Some of the other things that can happen that you need to think about are credit issues. We find one of the most common tactics by abusers is to ruin a victim's credit. And so then, if you've got commingled credit, if the abuser's criminal records get comingled with her records in some way, or his records if he's the victim, those are really challenging things that can have devastating consequences.

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 the AOL search data set. Are you a victim of domestic violence? And of course, she was, and how crazy that would be to have a reporter call up and say, hey, I've figured you out. Are you a victim?

And given the stigma that is still out there, that is incredibly concerning. Some of the other things to think about is not just physical harm, but some of the data that victims are most concerned about is their home address. And so when medical records started becoming a real issue, one of the things people were caught up on is the sensitivity of what's in a medical record, diagnoses, medical treatment, and of course, that's true.

But for a victim of domestic violence or stalking who's literally on the run or living and hiding or trying to rebuild a life, just the home address being compromised, shared in any way, either through legitimate or illegitimate means, that could put a victim's life in danger. And then, they may have to move. And so when you talk about cost, it's physical cost of relocation, of plane tickets, bus tickets, movers, alarm systems, changing door locks, slashed tires. So those are the types of things that we see when there's privacy and security breaches.

JACQUELINE CONNOR: Thank you, Cindy. And last but not least, Heather. Given your experiences, what kind of injuries result from the disclosure of medical information, sexual orientation, or gender identity that a consumer prefers to keep private? And then to go beyond that, what are the effects when people fear that this medical information, sexual orientation, or gender identity may be disclosed?

HEATHER WYDRA: Thanks very much for having me here. I'm happy to talk about these issues. I am an attorney at Whitman-Walker Health. We are a medical-legal partnership where we provide medical services to anyone living with HIV in the greater DC community and anybody identifying as LGBTQ, again, in the greater DC community.

So the reason that brings me here to this panel is because a large part of what I do in the Legal Services Program is to counsel and represent people who have been affected by a disclosure of personal information. A disclosure of, for example, personal health information, private health information, or a disclosure of gender identity and sexual orientation that the person did not want to be disclosed.

And I see people harmed by these disclosures in countless context, but the three I'll talk about today are in the work place, at places of public accommodation, and then in an interference with personal relationships, and that can be in the home, in the community, in the workplace, and elsewhere. So to begin to talk about the workplace, a large part of what I do is employment discrimination. And a lot of times discrimination starts when somebody's health information, in a lot of cases with the clients that I work with, it's HIV, it could be something else, is disclosed in the workplace.

And sometimes the disclosure is necessary. Sometimes it isn't. But regardless, the results are not always positive. And the negative effects can be seen in every aspect, at every stage of the employment relationship. I have had clients who have come to me who have gotten through the initial portions of a job application.

And then as you get a little bit further in the process, when you have what's called a conditional offer of employment, the employer is then allowed to ask for health information, can ask about HIV status and can even make people undergo an HIV test as long as everyone who was applying for that position is required to do the same thing. An employer can't pick and choose. And then, believe it or not it still happens, after that testing occurs, after somebody's status is public, they find themselves suddenly without a job offer.

That's illegal, of course it's illegal. But sometimes it still happens. And then it becomes my job to prove that the withdrawal of the offer was based on the HIV and not for some other purpose. That's a blatant example. Another one that can be more subtle but still happens is I worked with a client who was applying to be a bus driver in one of our nearby counties and, again, had to fill out a huge medical questionnaire.

It didn't actually ask about HIV, although it could have, that would have been permissible. She ended up disclosing it just because she had some blood work that was coming back oddly and thought, well, maybe if I just say this, this will end all of the inquisition. But the doctor, instead of saying, OK, now I understand-- she had letters from her personal physicians clearing her to do this job-- said, well, I want you to go back and get these three tests. And I need all of these records. And eventually, my client said, they don't want me here. And I don't want this job. They don't want me here.

So that's another example. And then, the example that I really see the most is someone who's going about their day doing their job. I worked recently with somebody who is a maintenance worker in an apartment complex. And because he had to take so much time off for doctor's appointments, he finally said to his supervisor, I'm positive. I've got to go to the doctor. I've got to get blood work. I have to have these medications checks.

Well, he didn't get fired. But all of a sudden, nobody wanted to work with him anymore. And he was put on these assignments by himself. And people said strange things to him like, shouldn't you be wearing gloves? And day after day, there was just some little indignity that he had to endure. So in that kind of thing, there's a hostile work environment claim that we can bring, but it can be hard to find a remedy for that. And it's just something that he had to endure.

So the next context that I'll talk about where I see harm occurring is in what we call places of public accommodation, so that is any place that people go, restaurants, hotels, gyms. The example I'm going to talk about is a gym. And I'm going to use the example of somebody who 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.

JACQUELINE CONNOR: We've been talking a bit about the actual injuries that come after the fact. And we've heard a little bit about the risks of injuries. But I guess for Heather and Cindy, I'm wondering if the people that you work with, if you see them acting differently? Or are they afraid to give and use their information for positive purposes to help them because they're afraid it's going to be misused in some way?

HEATHER WYDRA: I can start with that, and Cindy I'm sure you'll have plenty to add. Absolutely. Where I will see that a lot is in the area of health care, especially people who have experienced discrimination someplace else will be afraid to go and see a doctor because they're worried that either a doctor won't want to treat them because they're HIV positive, and yes, that still does happen, or someone who is transgender feels like a doctor won't know what to do with me. They'll be biased against me.

There are plenty of instances of doctors being very culturally insensitive to someone who is transgender and not understanding at all what their particular medical needs are or even why someone would be transgender. So yes, that is one area where I see people being afraid to go for health care outside of Whitman-Walker.

CINDY SOUTHWORTH: There's a real conundrum. I know some of the temps for data security have been to mail things to people's homes, that came up during some of the pretexting of phone records dilemmas. And from a domestic violence victim standpoint, that's not necessarily helpful. Same sort of scenario of somebody being afraid to go get health care after a victim's relocated to a different town because the health insurance will send notification of the care that was provided and the location of where it was provided to the original home address.

And it's really hard as it is to safety plan with victims of domestic violence and stalking who are trying to relocate and talk about, make sure that you grab the birth certificates, get the favorite teddy bear, make sure you've got the bank records and all this, and by the way, you need to notify the insurance company, this data broker, all of these other places and change your address. People are a little busy running for their lives to do all of those steps.

So what on one hand is an attempt to be providing transparent notification to the address on record, it gets very challenging. In terms of other places where victims opt out of society, what Damon was showing in terms of after people are targeted, do they shut down their Facebook accounts? Do they opt out of social media? Do they choose to exclude themselves? Or are they told explicitly?

We've had many survivors told by law enforcement, if you don't want to be threatened by your ex, well, just get off Twitter or get off Facebook, which is isolating, especially if your entire family is-- one of the ways that my family now communicates is- I know who's expecting a baby, because I'm on Facebook with all of my cousins and relatives. Telling me the only way I can be safe to be female in the world is to get off the internet because misogyny just happens, so get over it and just get offline, that's not possible. And it's isolating. It also impacts job possibilities. If I can't safely use technology, I am far less likely to get a well-paying job.

PAMELA DIXON: I'd like to add on to that just very briefly. The other thing that I see a lot in my work is that people don't understand what it is that will actually protect them, meaningfully, as opposed to things that they just feel like will protect them. A really good example of this are people who have had some kind of exposure that's problematic. And in order to reduce the information flows, I often recommend them to actually opt out of certain web sites. They won't do it because they don't want to give any additional information.

So I've actually had people who refused to opt out of, for example, financial information sharing because they don't want to give their social security number. People are so afraid of giving their social security number when in that instance, it would actually help them. So I do think that there needs to be a lot better understanding of, what piece of information can I give up that will actually help me? What pieces of information will genuinely be harmful? I'm not persuaded that getting off of all technology is the right answer here. I would really like to take the position that 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 exist, they come under the state, local, and federal anti-discrimination laws. So that could be Title VII, that could be the Americans with Disabilities Act, and then the state counterparts, the DC Human Rights Act, the Maryland Civil Rights Act and so forth. So that's one way for people to get a remedy.

For the disclosure of medical information by a health care provider, there is HIPAA. But for those of you who know anything about HIPAA, it doesn't provide a remedy to the individual who has been harmed by the disclosure. It can provide a penalty and sanctions and other types of punishments to the medical provider or the insurance company. But the person who has been harmed, there is no remedy for them.

And then, of course, there are some things that no amount of money compensates for. You try with loss of reputation, emotional harm and suffering. Certainly, yes, we try and fix those things with financial remedies, but there are some things that can just never go back to the way they were before.

LAUREN SMITH: So I think part of why we undertook this exercise is to understand that depending on the type of harm, it may have a different set of remedies. So for some of the more well-defined harms, such as employment discrimination-- so even if there is existing law saying that a certain group cannot be discriminated against in this context, technology can enable that to happen anyway where data could be used as proxies.

So you may not be able to not hire someone based on their race, but if you know what type of shampoo they use based on their online purchasing history or browsing history, that shampoo could be used as a proxy for race. So I think with some of these, we need to think about different methods to ensure that we are making sure that data are not being used as proxies for protected classes. I think that is a very clear, top level approach to preventing some of these harms. But ensuring that is built in to how we're thinking about these issues writ large, and that there are technological solutions to some of these algorithmic design to consider whether protected status should be used as an input in certain contexts.

And sometimes, it may be helpful to include protected class status, so that it could be checked to ensure that decisions are not being made based on that. But it also may be important to consider how it's being used throughout the process. And then, when you get down to less crisply defined harms, it's important to think about-- in some of the conversations recently, are we calling on 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 harassment stuff, like the doxing that I showed you. It's hard to point at a law that currently exists that would outlaw that type of behavior. And as the FTC showed, they had to creatively go after these revenge porn sites. And then finally, the states are stepping up in piecemeal enacting laws. But there's a huge gap in terms of understanding the laws defining non-consentual posting of people's information online.

PAMELA DIXON: I'd like to focus on one of the harms that is very, very tied to medical forms of identity theft, which is very aggressive, unethical, and often illegal, medical debt collection. So individuals who have written in complaints, both to the FTC and the CFPB, have routinely stated that they are working to get debt collections off of their credit bureau files for one, two, and three years. And there's narratives, actually, in the report we just put out of victims of medical identity theft who literally cannot buy homes and cannot move on with their life because they're being held hostage by debt collectors.

And some of the debt collectors will even tell them, if you just pay us $200 on this debt, we'll let you go. It's just a horrifying mechanism. And I do think it would not be a profoundly expensive item to fix to really take a closer look at medical collections and really clean up that niche of a sector. I think it's an area that causes a lot of harms to a lot of folks over extended periods of time.

DANIEL WOOD: Well, this has been incredibly interesting, and I think we could go on all day. But we promised that we'd leave some time for audience questions. So we have two questions from the audience. And the first one, I guess, is addressed generally to the panel. They're both addressed generally to the panel. So it is, can the panel speak to how to characterize the lower level of informational harms that exist and affect day-to-day life, but don't rise to the level that is being discussed by the panel. Anyone?

PAMELA DIXON: I wish we could ask a follow-up question to find out more about what they meant. Information annoyances beleaguer all of us. And it really does take discernment to figure out, is this annoying, or is this a problem? Some of the doxing and the spyware, these are large problems, but they may start as smaller ones. I think that this is a difficult question without knowing more from the asker, I apologize.

DAMON MCCOY: And you can clearly point at the targeted advertisements and things like that, ads showing up in people's pages that are clearly revealing other things that they're searching.

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 necessarily hurting you, but just circulating about you, you have to learn how to shut down some of the financial data flows.

It's easy to do. There's a lot of opt outs. But I do think that's a general annoyance that filters through all of our lives, unless you, of course, want to pay cash for absolutely everything. And I don't know anyone, really, who's able to do that anymore. It's just not a very easy way to live.

DANIEL WOOD: Anybody else? Or should we move on to the second question? So the second question is, to what extent are the harms experienced in these events surely due to the actions of a miscreant versus the negligence of a data steward?

CINDY SOUTHWORTH: I can jump in on this one. I think that is the million dollar question. I would say, the easy bad actors for me are the ones, like Remote Spy, that were actually advertising to allow you to spy on anyone from anywhere, that's just an easy lift of, they're pretty much malintended. I think where it's more challenging is if my information is compromised through a fairly innocuous minor data breach, does that information identify something about me that then has later long-term impact?

Do I not get hired because of my history of domestic violence, or sexual assault, or whatever stigma might be, because of something that was accidentally leaked and then makes its way through the stratosphere. I think the blatant bad actors are easy targets for us to point to. But I do think there are unintended consequences of breaches that, at least my constituency, runs into.

LAUREN SMITH: And I think the reality is that personalization has become a service, and something that we're very used to seeing on online platforms and technology devices that we use. And there's a lot of benefit there to consumers, but it also leads to downstream impacts. And so just as there is more data built on an individual, if that information is used in a way that an individual does not know about and would not prefer, then that could be perceived as a harm to them, and that could have, depending on the type of harm, either slight or significant impact on their lives.

And again, I think some of these questions are not settled questions. Is having the set of information that is presented to you when you log into an online platform personalized to you based on what your friends like, based on what you've shopped for, that may provide you with a great service that you really enjoy, but it also could be used in other ways that you may not prefer. And so I think some of these harms we're still just starting to understand. And as much transparency and control that consumers are able to have, I think the more we're able to safeguard in the long run how they play out.

DANIEL WOOD: Anyone else? Well, I guess we have about a minute each for final thoughts from the panelists. Can we just start with Pamela?

CINDY SOUTHWORTH: Not being a legal expert, but instead talking about very pragmatic things, I loved the example that Damon used about how technology filtering can make such a difference to somebody's online experience and help mitigate harassment. We've seen very pragmatic approaches to information harms in my 27 years of doing this work. One was a domestic violence shelter years ago that their address was accidentally published by the local phone company. And the phone company paid off their mortgage and helped them move, not a light lift but very practical and very pragmatic.

I think the granular attempts to allow people to control over their own experiences, such as filtering comments within Instagram, Facebook, Google's working on it, will help people be able to stay online and have less assault and harassment coming at them.

DANIEL WOOD: Thank you. Other final thoughts?

PAMELA DIXON: I have a comment about solutions. Very often I hear people talking about solutions, and well, we're going to solve our medical identity theft problem by installing a biometric system to make sure all these patients are who they say they are. Meanwhile, they've got a huge security problem in their biometric system. It is just not possible to find a single, silver bullet, gorgeous, perfectly formed solution that will solve 100% of an informational problem. It doesn't exist.

We have to look at layers. We have to look at different facets. We've got to have a multifactorial approach to any kind of problem that we're trying to solve. And I really like the idea of collaboration across states and federal agencies. I like the idea of collaboration amongst different expertises and against different types of victims and a variety of stakeholders.

I think it's an important approach. It gets a lot of ideas on the table. And it avoids the dangers of the quick, easy solution. I always like to say the absolute longest distance in the world is a shortcut. You've got to take the time to find the nuances in the solutions, or it's just going to be a disaster.

DAMON MCCOY: I'll echo what Pamela said is that I think we really do have to put a lot of effort into trying to understand and measure the kinds of harms that are going on and get a good grasp of these measurements because when we start deploying solutions, it's going to be impossible for us to say whether the solution actually helped or potentially harmed people unless we have these good, deep measurements of the kinds of harms and the scope of the harms that we're dealing with.

HEATHER WYDRA: And I'll make a final remark. I've been actually impressed by the discussion here and its mix of technology but also compassion. And it's not necessarily what I would have expected from a panel at the FTC talking about these types of things, especially that a lot are computer-based and technology-based.

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.