FTC Spring Privacy Series: Mobile Device Tracking
February 19, 2014
Transcript

AMANDA KOULOUSIAS: Thank you all for coming today and welcome to our seminar today on mobile device tracking, which is the first in our series of spring privacy series seminars. My name is Amanda Koulousias and I'm an attorney here at the FTC in the division of privacy and identity protection. We're going to get started with our first presentation in a few minutes but first I just need to go over some housekeeping issues.

Anybody who goes outside the building without an FTC badge will be required to go through the magnetometer, an x-ray machine, prior to reentry into the conference center. In the event of a fire or evacuation of the building, please leave the building in an orderly fashion. Once outside of the building, you'll need to orient yourself to New Jersey Avenue. Across from the FTC is the Georgetown Law Center. Look to the right front sidewalk and that will be our rallying point. Everyone will rally by floors and you'll need to check in with the person accounting for everyone in the conference center which will likely be me or Kristen. So you could look for us.

In the event that it is safer to remain inside the building, you'll be told where to go. And if you spot any suspicious activity, please alert security. This event may be photographed, videotaped webcast, or otherwise recorded. By participating in this event you are agreeing that your image and anything you say or submit may be posted indefinitely at FTC.gov or on one of the Commission's publicly available social media sites.

For anybody who wants to submit questions today, we'll be taking question cards which are available in the hallway immediately outside of the conference room if you haven't gotten one yet. And if you have a question, just fill out your card, raise your hand, and someone will come and get it from you.

For those of you who are participating via the webcast, you can email your questions to mobiledevicetracking@FTC.gov, you can tweet it with the hashtag #FTCmobile, or you composed it to the FTC's Facebook page in the Workshop Status thread. Please understand that we may not be able to get to all questions, but we'll do our best to incorporate as many as we can.

Now we're going to get started today. First with a presentation by Ashkan Soltani who is going to give us a technical overview. Ashkan is an independent researcher and consultant who focuses on privacy, security, and behavioral economics. His research has examined the prevalence of online tracking and expose practices designed to circumvent consumer privacy choices. And he has previously served as staff technologist in the Division of Privacy and Identity Protection here at the FTC and also worked as the primary technical consultant on the Wall Street Journal's What They Know investigative series. Please welcome Ashkan.

ASHKAN SOLTANI: Hello. Hi, everyone. Glad you all made it this rainy day. I'm going to just quickly go over how some of this technology works and then let people jump on in the panel and some of the specifics. It's going to be a very kind of high level overview, but feel free to ask any questions or any clarifications.

So panels on mobile device tracking. I'm going to speak about location aware devices and then I'm going to speak about device aware locations. And then kind of touch on some of the benefits and some of the concerns from a technical perspective.

So we're talking about mobile phones, generally. Smartphones more than kind of traditional phones or the traditional phones, feature phones, still kind of fall into space. And we're kind of probably all aware of location aware devices now. So most of our smartphones allow us to find where we're-- map our location or find restaurants. The device itself collects its location from a variety of sources. So via a GPS antenna that's on the device that talks-- position itself on the globe based on satellites in the sky, via local Wi-Fi signals that allow it to triangulate and query against databases like Google and Apple to tell it where it's approximately located, and via the cell towers-- the mobile providers like AT&T and Verizon allow the devices to triangulate their location and then do queries like, what are the restaurants in my area?

This is a kind of quick overview that I provided to a Senate panel about two years ago, but it's kind of generally describes all the way the device collects location and puts it onto the device. We've done with what they are series and the FTC has also done a lot of reviews on what apps collect and what apps collect location. This might be kind of old news to you but oftentimes an app will collect location to tell you where a restaurant is, but then it might share it with a third party ad networks or share it with other entities to ether benefit the user or to provide advertising.

And location-- generally, when we say location it can mean a number of things. GPS location can be accurate down to 100 feet or even, depending on the technology used, Wi-Fi is often accurate to a city block level. But generally-- and I thing the FTC has some nice definitions of what location is in there. COPPA-- I think the COPPA guidelines describe location down to a city intersection. Generally we mean where you are relative to a map.

And one technology that I didn't talk about in the earlier slide of the Senate hearing is kind of a newer technology called Bluetooth Low Energy which isn't very flashy so iBeacons is often what it refers to them and other people have referred to. And this is, essentially, another way for a device to determine its location based on low energy Bluetooth signals from beacons at stores or you yourself could purchase and put. So you could buy a beacon at your home and when your device encounters that beacon, you could set it to do something.

One of the common uses here is, oftentimes, stores might-- are starting to roll out beacons that would allow you to, when you pass an item in a display, give you an alert when you pass by that system to say, hey, this item is on sale or here's a coupon. The technology works, essentially, by the Bluetooth antenna in your device monitoring what other Bluetooth devices are around it. And then once that's detected, it will signal a particular message or a particular website or a particular action on your phone. And they are often very accurate down to five meters or less. And it depends on the specific make of the device. And they're often-- they're starting to be rolled out in stores.

The other thing that's starting to be more commonly rolled out in stores or a class of store is device aware stores or device aware locations. This is an example from a Cisco interface about a particular interface for a mall to allow the mall to identify where users are traveling, what stores

they're traveling to, and what displays they're looking at. So this would be an example of a device aware location.

In fact sweetgreen here-- many of us go to sweetgreen for salads-- sweetgreen is a device aware location. It, I think, partners with Nomi to identify what devices come to the store, how long they stand in front of the register, what devices might be repeat customers, for example. So if you've got to one sweetgreen and then later come back to another sweetgreen.

As I said, when your smartphone kind of tries to determine its location, it's actually a two way signal. So often Bluetooth and cell tower location services are two way, both the devices receiving as well as the device transmitting. And by transmitting, the signals that the receiver receives essentially allow them to triangulate the location on the device.

Another way to look at your device is actually a series of transmitting antennas, right? So a typical smartphone will have a Bluetooth antenna, a Wi-Fi antenna, a GPS antenna which is for receiving, typically, and then a GSM antenna, the antenna that you use to speak to AT&T or T-Mobile or whoever your provider.

And each of those antennas emit signals and in those signals the provider, for example, is able to triangulate the location of the device. So here Verizon and AT&T, based on its network of cell towers, can tell either which cell tower you're closest to or triangulate a more accurate position based on the distance between towers. And this is based just by your phone being on and sending beacons to the network saying, hey, I need cell phone signal or what signal is near me? Or when you use the phone.

So this can happen just by the device being on. Similarly, there are companies like Path Intelligence that intercept those same signals that Verizon or AT&T receives to also perform triangulation of your device. So this is-- the antenna in the top right corner is a device that Path Intelligence sells that malls and other stores can place in their mall and, essentially, as your phone is becoming to AT&T or T-Mobile or whoever, these devices also pick up the phone's identifier and its location or approximate location in the mall.

Bluetooth happens the same way. So as your device tries to look for a Bluetooth signal or is communicating to Bluetooth and Wi-Fi signal, Wi-Fi networks, the device is transmitting basically a beacon or a frame looking and essentially trying to identify nearby networks. There are companies, I think some here today, that also intercept those beacons, those signals, and provide geolocation services based on your Wi-Fi, Wi-Fi emanations.

And this can happen either when the device is on a network, it could happen by the network you're on-- so if you go to a hot spot, oftentimes the hot spot might have this feature built in-- or this can happen independent. So you can go to Starbucks and Starbucks might have a Starbucks Wi-Fi network, but they might also feature one of these devices to also triangulate your device based on your communications to the Starbucks network.

There's a variety of methods. I kind of just touched on a couple. Your phone might have other antennas like NFC or RFID. This is a schema from an open research paper about magnetic and

LED lighting based location detection. So emanations from your phone's LEDs or magnetic field that it emits. I'll say, the more kind of developed ones that I know about are the cell tower based and Wi-Fi based location technologies, as well as the Bluetooth iBeacon type technologies.

The question is, how do you identify a user or what is identification in this? Are they tracking you by name? How do they identify the same device to where it comes back to the store? And the key to remember is, each of these antennas that we talked about on the device-- the Wi-Fi antenna, the GSM antenna, the Bluetooth antenna-- they all have a unique serial number, a globally unique identification. This is kind of like your social security number but it's specific to the chipset on your phone. So it's designed to be globally unique such that no other person or no other device has that same number.

And it allows them to uniquely identify that device. So it might not refer to the device by name, but it will say, for example, you can ascertain whether it's an i device an iPhone device, an Apple device, or an Android device from this information, as well as whether it was the same device that you saw yesterday. And, essentially, this device, while it doesn't reveal perhaps the owner's information directly, it kind of helps to indicate what the location habits of a particular device are. So you can say, this device travels through these set of cell towers at a given time, or this device has come to sweetgreen before yesterday, or it went to a different sweetgreen store last week. And it allows, essentially, to refer to the device uniquely.

One thing to remember is those serial numbers are persistent to the device, their hardware serial numbers. There's actually very little users can do to delete or change them. In fact, there was a bill last week-- I think Schumer was trying to propose-- to make it illegal to change some of these such that when phones are stolen they could be blacklisted based on this information. So as long as you have a device, this information is persistent to the device. So it's a pretty reliable or robust identifier.

And sometimes-- oftentimes you might hear of the device identified as being hashed. Hashing is just a mathematical algorithm you can apply to a particular identifier. So that top line-- the one beginning with E8th-- that's my particular MAC address for one of my devices. And the bottom, the number starting with 4-8, is the hashed version of that identifier. And the key with hashing is that it kind of obfuscates the number. So it's very hard to go back from the hash number to the Mac address, the original Mac address. But you're guaranteed to always get the same outcome.

So any time you see my device and you hash with the same algorithm-- in this case, this is a SHA-256 hash-- you will get the same outcome. And so what's key here is, again, the hash identifier, while it's not revealing the actual identifier, it's still another robust, unique, or globally unique identifier. It's just as robust as the Wi-Fi address.

Actually, there was a great blog post by Ed Felton, I think last year, about whether hashing makes data anonymous. And he goes into great detail about how this works and the fact that hashing doesn't make it anonymous it just basically transforms it from one identifier to another, but it's still a robust identifier.

And another way to-- there was a response-- for example, Euclid Elements is one of the analytics companies that do Wi-Fi analytics-- they would argue that this information is anonymous. It's very difficult to identify people and they say this doesn't refer to an individual. But in response to a series of letters from Senator Al Franken, they responded that, yes, if you provided a device to law enforcement or if law enforcement provided them with a device, they could perhaps tell what other locations that device had been.

So you're able to get from a device to historical location even if the information is hashed. So that's something to be mindful of. So it's anonymous in the sense that it doesn't refer to a person by name. It's hashed in that it might obfuscate their original Mac address, but you can still provide historic device location based on some of these identifiers even if they're hashed.

And oftentimes these things are used for-- what are the benefits of these technologies? Well, one of the big benefits is coupons, for example. Everyone loves coupons. Or you might be able to quickly see a deal that's happening near you or maybe find a location of your receipt. There's actually a great number of use cases where this is helpful both from the consumer side as well the retail side.

The retailers can, for example, use the technology to identify what stores are popular, what displays are popular, where users are going, whether there's repeat customers. They can use the information to determine how queues are progressing, whether people stand in line too long and, if after five minutes you jump out of line, you might want to add another queue.

But there's also a number of concerns with this technology, which I'm sure the panel will get into, but just to touch on them briefly. This information can be sensitive in the sense that it can provide demographic information about people's age. There's no way, for example, to tell whether it's a kids device you're tracking or an adult's device you're tracking. Based on the types of other locations you've been going to, you might be able to infer demographic information like lifestyle interests.

This is a company, Turnstyle, that provides demographic interests in the bottom right about nightclubs and music and any particular interests. You can infer, just like behavioral advertising, you can infer interest based on people's location behaviors as well.

The other kind of-- this is Verizon's analytics. Verizon is a carrier. They provide their-- I think it's called Precision Insights-- and this is, for example, a tale of people's activities in one city. An aggregate, but how people spend their day. Whether they go to have hot dogs in the morning or whether they go to the top five restaurants they go to. And this is essentially aggregate analytics but it provides a big picture of people's day. Right?

So they can track-- for example, T-Mobile or Verizon know how you spent your entire day in terms of the locations you went and so that might be a concern to some people. And the general class of concerns are that-- like most other tracking debates-- it's essentially that the collection is invisible, passive. People need to opt out versus opt in. How difficult it is to opt out. So Joel's group have provided an opt out system that lets you, for example, provide your Mac address to

this network to create a black list of people who want to not be tracked. That's kind of difficult for most users, I suspect, to go and find their Mac address.

There's probably going to be iterations on this. One idea I had was, for example, to set up opt out Wi-Fi network at each location such that a user can just join that network for brief instance, and that network can capture the Wi-Fi address. Kind of like what Tanya is doing outside. So you briefly join an opt out network, it catches your Mac address, adds you to the opt out list and kicks you off the network. That could be done in a few minutes by Seth or myself using some Open Source software.

And that would be, maybe, an easier way. But it's still a difficult process. Users have to know that it's happening. It's the typical tracking debate.

We touched on how the identifiers might not be fully anonymous or they're pseudo anonymous. And then one of the big issues, I think, is that the retention period of even the pseudo anonymous tracking information is unclear. So whether law enforcement or other divorce attorneys or whoever can get this information might be a concern.

Convergence, finally, is one of the areas that are kind of potentially sensitive. This is Turnstyle-- sorry, this is RetailNext and they, for example, combine your location history, Wi-Fi activity, point of sale activity, payment cards, et cetera to provide a more concrete picture of the user and the user experience. And so as you combine things like location with other types of activity like tracking or things where you might-- sorry, like purchases where you might identify yourself or use a credit card or sign up for a mailing list, I think people will find that the location information combined with information about them might also be sensitive.

This is just an example I just ran the other night where CVS provides a mobile app to let you find coupons and find your store. But it transmits your hashed identifier. That's my hashed identifier we saw earlier in that SHA-56 algorithm. The app itself sends home or phones home your Mac address to CVS. And Apple's trying to curb this behavior but on the Android platform this still happens.

And so this information about my usage of the app, my signing into the app, can be combined with some of the other analytics like the retail location tracking to get a better picture of who I am and what stores I go to. So that's the general kind of landscape of how this stuff works. Be happy to take some questions.

AMANDA KOULOUSIAS: Yeah. If anyone in the audience has any questions, feel free to fill out your question cards and somebody will come and get that for you. And we can ask those. Just to get started, Ashkan, I had a quick question on-- so you talked about the different ways that companies can do some of this and you talked about both the Wi-Fi and the GSM interception. Can you give us a little bit of insight into why a company might want to use one or the other?

ASHKAN SOLTANI: So, sure. GSM based, cell tower based location analytics usually can be collected by your carrier-- so the AT&T and Verizon's as well as companies like Path Intelligence that have these antennas. They're, essentially, collection devices that intercept your

communication to your carrier. This is a pretty robust way to track users because oftentimes your phone is always connected to your provider. So unlike Wi-Fi beacons, you might not have your Wi-Fi antenna on or you might not be using it. Whereas you're GSM often sends a heartbeat every-- depends on the carrier-- but a pretty regular interval pinging the tower to identify what tower you're associated to. So it becomes a pretty robust way to track individuals.

Additionally, the GSM protocol requires one of the identifiers to-- there's a persistent identifier but there's a second identifier which is often the one used to track individuals called the TIMZ. These rotate at some interval but my understanding is that they can be kind of persistent for up to 30 days. So it provides a good picture on a person's location habits over 30 days and whether they come to the same store or not. It's a good signal in the sense that most people don't turn off their phones.

AMANDA KOULOUSIAS: And what about Bluetooth?

ASHKAN SOLTANI: So Bluetooth is a more-- I would argue most people, or not as many people, leave their Bluetooth antennas on. I think the panel can speak to what the prevalence and penetration of this stuff is. I would argue in the grand scheme of antennas you have the GSM antenna which is almost always on, Wi-Fi antenna which is, if it's on, is beaconing and maybe not connected to a network, and then Bluetooth often is low energy and the distance is lower. But it provides some additional benefits in that the resolution is much more fine grained. You can actually have much more-- you can say whether I'm next to you versus the other end of the table pretty accurately. So Bluetooth has some benefits in this context.

AMANDA KOULOUSIAS: OK. And does it also go in that order? GSM, Wi-Fi and then Bluetooth in terms of how popular each of those technologies is right now?

ASHKAN SOLTANI: I would argue-- at least I know of more companies that are doing Wi-Fi based partially because I think it's potentially cheaper, it's potentially more-- I think the laws also a little clearer on interception of Wi-Fi signal versus interception of GSM signal. But I think the panel could probably speak to that.

AMANDA KOULOUSIAS: Well, it looks like we've got about a minute left so I think we've got time for one question that we've gotten from the audience which says-- somebody has asked-- they said they assume that there are multiple hashing algorithms and to aggregate data for a phone across multiple locations they assume all locations would need to hash the same way or use the same analytic form. Is that true?

ASHKAN SOLTANI: That's right. So the hashing-- a hash is essentially a transform. You could hash my name by adding one character to the end of my name or changing my name by one letter. And everyone would have to agree on that hash for them to be able to synchronize data. One thing that's missed, I think, in a lot of the hashing debates bases is that, oftentimes, the technology is now there where we can-- while it's difficult to reverse-- so while it's difficult to take a hashed identifier and go back to my Mac address, you can essentially innumerate the list of all Mac addresses and all hashes under a set of hashes. This is called a rainbow table.

And this is-- I'm sure people have been following the recent Target breaches and all the other breaches. This is how hackers will determine your password. It's very difficult to go back from a hash, but you can say my name always ends up in this hash pre-computed ahead of time and they'll look for a match.

So, yes, to the question. Retailers would need to be using the same hashing algorithm to coordinate across different retail collection points. My understanding is the popular ones are SHA, SHA-256, Sum MD5 and so-- but even if they don't, it is still possible to reverse engineer what the original information was.

AMANDA KOULOUSIAS: We've got one more question. It looks like we're running out of time so if you could answer this--

ASHKAN SOLTANI: Sure.

AMANDA KOULOUSIAS: --really quickly and then we'll get to it in more detail on the panel, I think. But somebody has asked, can you just briefly discuss security hacking concerns with Wi-Fi and Bluetooth?

ASHKAN SOLTANI: Sure. So I think one of the issues with Wi-Fi is that it's not a private identifier. It's kind of the same issue of social security number. Both my app can know my Wi-Fi, the network around me can know my Wi-Fi, the ad network can know my Wi-Fi. And so as people are using Wi-Fi as a robust identifier, it's just good to know that, for example, lots of people-- Latanya outside knows your Wi-Fi identifier-- and so if people making associations to that then it's potentially problematic from a privacy and security perspective.

AMANDA KOULOUSIAS: Great. Thank you very much. We'll invite our panelists to come on up.

KRISTEN ANDERSON: All right. We're in the process of trying to turn the air down in here so that we can be heard a little bit more clearly. So I apologize if anybody couldn't hear what we were saying earlier. My name is Kristen Anderson. I'm also an attorney in the Division of Privacy and Identity Protection and Amanda Koulousias and I will be co-moderating this panel. As a reminder of how to submit questions. If you're in our live audience you can fill out a question card and someone will come around and get that. We may be taking them throughout but we'll definitely take them at the end. And if you are watching via webcast, you can submit your question via email to mobiledevicetracking@FTC.gov, you can tweet it to #FTCmobile, or post it to the FTC Facebook page in the Workshop Status thread.

So now we'll begin our panel. When we put together panels like these, we try to include as many different perspectives as possible so that we can evaluate these emerging technologies from different angles. Today we're joined by, starting at my left, Ilana Westerman. She's the CEO and co-founder of Create with Context, a digital innovation firm focused on strategic research and

design. She's responsible for corporate development as well hands on client work, including research, innovation and design.

Next we have James Riesenbach who has built and led wide ranging digital media marketing and analytics businesses for over 25 years. He's been the CEO at iInside since January of 2013 after previously serving as strategic adviser to the firm. Next we have Seth Schoen who's a senior staff technologist at the Electronic Frontier Foundation where he's worked since 2001 promoting understanding of the implications of technology for individual rights.

Next we have Mallory Duncan who has served as senior vice president and general counsel for the National Retail Federation for more than 15 years. He's responsible for coordinating strategic legislative and regulatory initiatives involving customer data privacy, financial services and consumer protection. And finally, we have Glenn Tinley who founded MEXIA with the focused vision to help companies understand how the changing dynamics of an increasingly online world impact consumer behaviors at brick and mortar locations, and how consumer experiences can be improved by understanding these behaviors. Before we get started, I'll have Seth just very briefly provide an overview of what the Electronic Frontier Foundation is and what its interest is in mobile device tracking.

SETH SCHOEN: Thanks. The Electronic Frontier Foundation is a nonprofit advocacy organization based in San Francisco. We actually have one lawyer who works here in DC but dozens of people out in San Francisco. We're interested in the implications of technology for individual rights including privacy. And we tend to think of location as one of the most sensitive forms of personal information because of the way that it implicates all the other kinds of personal information. And I can talk more about that but it's sort of the meta personal information because you can use it to do so many other kinds of things. So we're interested in the implications of location tracking for personal privacy in that respect.

AMANDA KOULOUSIAS: Thanks, Seth. Ilana, if you could just briefly introduce yourself and Create with Context.

ILANA WESTERMAN: Sure. Ilana Westerman, Create with Context. We are an experience design firm. So what we do is we design user experiences for digital devices. So anything from mobile to web to wearables. Anything that has a digital interface.

And what we really do is to try to understand the consumer first. What do they care about, what are they doing, what do they need, what do they want? And based on that, that's how we do our design. So it's a data driven design process.

KRISTEN ANDERSON: Thank you. And to get us started we'll just have Glenn from MEXIA and Jim from iInside. If you can just each take a few minutes to describe the service and technologies that your company's offer and the kinds of insights they're providing to retailers and your customers.

JAMES RIESENBACH: Sure. Well, good morning and it's a pleasure to be here. iInside is a technology company that's been in the business of creating location based services for many

years now. But our focus has moved, over the recent years, to creating technologies that help our clients-- which are primarily retailers-- better understand how to improve the customer service and customer experience and their operations. And also, at the end of the day, help them to compete more effectively against the growth of e-commerce companies that have compromised and made it a little bit more difficult to compete in today's retail brick and mortar environment.

So we provide a variety of tools. Everything we do is aggregated. We view ourselves as part of a continuum of marketing research companies that have been out there for many, many years providing insights based on statistical samples of data. We're not in the business of looking at individual consumers or trying to provide individual insights. We're in the business of providing aggregated views that help our clients compete more effectively.

GLENN TINLEY: And MEXIA Interactive, somewhat similar to iInside, we're a location analytics firm. So we capture data for our clients based, again, on aggregate collection of that data. That helps our clients understand what is happening within their locations. Our core belief is that we want to give them the advantage and help them understand those behaviors so that they have the added benefit of understanding what is happening online and being able to compare it on location or within those locations.

Our clients primarily are airports, shopping centers and large retailers who all are trying to understand what they can do better to help the consumer experience and make that more effective, more efficient for consumers when they are in a location. And we work specifically with clients on one to one basis to analyze that behavior and anonymize it in multiple different fashions so that there is no combining or profiling to be happening within any of the deliverables that we're providing.

KRISTEN ANDERSON: Could each you talk a little bit about what exact technology you're using to provide those services?

JAMES RIESENBACH: Sure. What we do is we will work both with the retailers existing technology if they have Wi-Fi access points that are used for public Wi-Fi to allow them to provide Wi-Fi to consumers. That those sources of hardware can also hold the data and help us to aggregate it. And we also have our own hardware that we'll place throughout the store that utilizes a combination of Bluetooth and Wi-Fi to sample the shopper audience or in airports or other environments.

GLENN TINLEY: And, again, we're very similar. We can capture either a Bluetooth-- either what's called Bluetooth Classic or Bluetooth Low Energy-- as well as a Wi-Fi signal. We're a little bit different in that we only assemble and install our own hardware in facilities so we're not dependent on pre-existing installations of anything to capture the data. We're installing our own hardware in spaces based on deliverables of what the client is trying to achieve and depending on the granularity that they're trying to achieve.

KRISTEN ANDERSON: And are each of you also combining the data that comes from the Wi-Fi and the Bluetooth?

JAMES RIESENBACH: Yes. We combine it. What we try to do is deduplicate. So if we're seeing the same-- if we're seeing the same behaviors in multiple cases, we try to look just in aggregate. So we want to make sure that we're providing the most valid, statistically reliable samples that we can to our clients.

GLENN TINLEY: And I'll answer that a little bit differently. By combining if you mean combining within an individual client, we'll make sure that one device either has both-- if we capture both signals it's one device. But no data is ever combined with other clients. So I just want to make-- be clear about that. We're not combining data amongst clients. It's always within an existing client.

JAMES RIESENBACH: And that applies to us as well.

KRISTEN ANDERSON: Great. Thanks.

AMANDA KOULOUSIAS: Great. So, Mallory, if you could just give us a little bit of insight into what retailers are looking to gain from these technologies. Are there particular insights that are particularly important to NRF members and just some of their thoughts on this.

MALLORY DUNCAN: Sure. I'd be happy to. Let me just start by saying NRF represents a broad range of the retail industry from single store operators to some of the largest retailers in the US. And retailers, obviously, want to be successful, but to be successful they've got to do two things. First of all, they have to understand their customers. And secondly is they have to understand their stores. Now, that may sound very obvious but, in fact, it's very, very difficult to do in each case.

The first drives retailers to try to find, how do we deliver the services and the attention that our customers want so they will be encouraged to come back to that particular store? The second one, which is understanding the store, is, how is your store laid out? How are things arranged in that store in such a way that people are attracted to it? How do people move through the store? And that can be factored by product selection, it's location within the store. And, necessarily, what are the avenues for loss? And so there's-- loss prevention is a big part of it.

We use these tools in order to increase our understanding of the stores and their operation. And when you do that, you're striking a balance. You're maximizing the stores effectiveness which increases your ability to compete with others. And at the same time, you can't go so far in doing it that you destroy the trust that's inherent in the first thing which is to bring people in so they want to shop in your store. So we are using these tools to try to find the best possible balance between those two.

AMANDA KOULOUSIAS: Great. And so, Jim and Glenn, you both mentioned the variety of insights that you can offer to retailers or other customers. I wondering if you can give us a little bit more detail about some of the particular insights that you offer. For example, are you looking at new versus returning customers? Are you able to tell who has actually entered as opposed to possibly walked by a location?

JAMES RIESENBACH: Yeah. There's a range of data that we're able to collect via our methodologies. The first is pathing. So we're able to look in aggregate at how shoppers move throughout the store. Retailers are using as many ways to optimize their store environments. We have many retailers-- one of the most expert expensive aspects of running a retail business is real estate and they want to understand where do shoppers go and how are they optimizing that environment both from a merchandising and marketing perspective, but also from a flow for customers so that customers are able to easily find what they're looking for. So pathing is very important.

The second one is dwell time. So we are able to look at, again, in aggregate, how many shoppers go into a particular department and what's the average time they spend in that department. Now, that helps them to understand-- the retailer to understand are they providing the right level of customer service, do they have to the right staffing at a particular time, are they providing the right products and the right mix of products side by side?

The third, and this is very important-- and this is both in retail and other environments-- is wait time. Our clients are very focused on providing the best throughput, if you will, at the cash registers and to basically assure that customers don't wait in line. One of our clients has a benchmark that they set that says two minutes is the maximum time that they want any customer to wait at a cash register. And so what we do is we help them say, over the course of a week, by day of week and time of day, these are the areas where your meeting your benchmarks and this is where you're not. And here's how you may have to reconsider. Do you open more lanes? Do you staff differently? So that's important.

And the final one that we're able to do is because of the way that we hash-- and Ashkan talked about this-- we can see the same device multiple times but, again, that's done in a way that will show a retailer, first of all, what percentage of shoppers came back to their store on a recurring basis. Many grocers and convenience stores are really interested in that because they want to understand how are they doing in customer loyalty and repeat visitation. And also even across the single chain.

Now, we don't share across different companies, but within the same chain-- a convenience store company, for instance-- might want to know, are their customers going to multiple stores within the same chain. So those are the basics of what we do. Glenn, I'm sure you have some others well.

GLENN TINLEY: Well, just touching a little bit on what Mallory had said is retailers and malls which are a collection of retailers are interested in-- they have departments that are set up to help them determine what products that are going to go across a chain of stores or a grouping of stores. So their interest in knowing are customer base spending time in certain aisles or around certain products in one area of the country where they may not be in a different area of the country. And that helps them to determine maybe is their product selection different or should it be different or should their product mix be different.

And by measuring whether or not, or collecting the data whether or not they're dwelling in specific aisles or by specific displays, and are customers then actually stopping at check outs?

Because that helps them to measure conversion of are people actually coming into the store and leaving without checking out. So product selection and where aisles are placed and how aisles are placed in stores are crucial understanding points for retailers.

In a shopping mall environment, the collection of retailers is very important. So how is our store mix set up? So we work with some mall clients who introduced a new store into one mall and they want to understand, are those customers that are going to the new mall, or the new store there, are they also going to other stores? Are they spending time in other stores? Or are they not visiting the new store? And if they're getting a positive amount of information from that, then they can look to expand the store, maybe across some of their other locations, some of their other mall locations.

These are decisions that affect millions of dollars in terms of real estate, in terms of leasing, product selection, product mix. And these are the decisions that this data is helping companies to make. All, again, in aggregate.

But one of the other things is in relation to staffing. We recently worked with a company-- mall company-- who we determined that they had security staff coming in at a specific time of day on a consistent basis across the network. And what we provided them with was you're traffic, what you think is happening or what you traditionally think is happening in that center, is shifted by about an hour and a half.

So they readjusted some of their staffing schedules of their security because they want to staff up more when they're required and they don't need as many on hand when there's less people. It's all based on ratio. And that is allowing them-- not currently right now-- but as they roll this out, they've estimated that this is about a quarter million dollar savings to their bottom line. So they're helping their bottom line but they're also making sure that their customers are getting the attention in terms of having staff on hand when ratios are requiring it.

So the customer experience is not necessarily impacted immediately there but it is because if something were to occur they know that they've got appropriate security staff on hand. So those are just different ways that taking the information, and it's general information based on patterns and movements and behavior, that is allowing them to then analyze that and make these decisions.

KRISTEN ANDERSON: I have a bit of a technical question. So with respect to the Wi-Fi and Bluetooth, are you-- whether it's tracking within a mall-- can you set it up so that you're only tracking within the common areas of the malls and not spilling over into the stores? Or, for individual retailers, can you ensure that the tracking is taking place just within the walls of the stores or does it spill out a little bit into the hallway? And how do you account for those things?

JAMES RIESENBACH: We're able to attenuate the devices so that we can, basically, either narrow or increase the range, depending on the goals and objectives. So we can actually, each individual piece of hardware, can have a range that we determine that says, we only want to track within this store or even within this department or even down to within this particular lane for

cash registers. And so we have a variety of technologies that allow us to geofence and block off other areas we don't want to see.

GLENN TINLEY: Very similar. In a mall environment or a large environment like that, naturally a signal is still a signal so there's certain amount of movement. But based on what the deliverable is in terms of maintaining signals within a common area, is how things are reported on.

AMANDA KOULOUSIAS: And so we've gotten a question. Both of you mentioned that one of the insights that you're able to offer is the new verses returning customer rate. And so, in order to determine that, how long do you keep that individual information to determine that?

GLENN TINLEY: Well, in terms of individual information, we're not reporting on specific devices, necessarily, that are returning. They're captured in an aggregate form so it's a percentage. What we report on is 12% of the customers in this store visit three times per month, 8% visit four times per month. So that's what's being reported and managed.

And the reason to do that is, a, to keep-- it is aggregate so it is percentages, or total number of counts of devices that are coming back in. So it's not this device. And some will say that, yes, you can still track it to-- or bring out, specify a specific device, but, in the end, our clients don't have access to that individual data. They have access to aggregate data. That data is automatically aggregated at the time it's collected and moved to a different set of servers. So it's not able to then highlight out a specific person.

JAMES RIESENBACH: The other thing that's important to recognize is that the turnover of mobile devices is frequent and increasing and, therefore, any device that is seen is going to have a limited lifespan, in general, as far as the use of that data because consumers upgrade a device and then we, basically, are going to see a completely new device. We obviously don't know who that consumer is or anything about them anyway. But that is one of the kind of self automatically refreshing aspects of the methodology.

SETH SCHOEN: So it seems like it would be useful to draw the distinction here between what you report to the retailer and what you, as the analytics provider, know. I think the intention of the person asking the question was, what do you as the analytics provider know? What information do you have as opposed to what information goes to your retail clients?

GLENN TINLEY: Well I guess there's two different things. So, two things. Our contracts are very specifically and purposefully set out that the data that is collected on an ongoing basis with our clients is our client's data. So we are legally and code of conduct obligated and contractually obligated that we don't go into that data to then determine-- the data belongs to our client. So we're not doing going back in to figure out specific, or pull out specific devices, as well as the data is still on an aggregate server. So it's being reported that way but, yes, as an analytics firm, I guess you could say that, yes, we have access to the data across. But we as a company do not combine any of that data and it belongs to the individual clients.

JAMES RIESENBACH: It's important to note that the only data that is stored by any of the companies that are signatories to the code of conduct are hashed Mac addresses. Now, we understand from Ashkan's presentation, is there a theoretical possibility that that could be used in a way that you could see a pattern from that same device? Sure, if there were a massive number of implementations across the entire universe. That's not really where the state of the industry and won't be for a long time to come.

What we have is a hash Mac address. So we don't actually store anything that's identifiable even to the specific device right now. And then, even for our own purposes, the only thing that we will do is use it against a statistical modeling methodology. So we never pretended or claimed to be a tracking company. We're a statistical modeling and marketing research company that provides profiles of what happens in the store based on relatively small sample size.

With Bluetooth-- and the question was raised earlier-- what percentage of the devices are actually seen when people go into a store? Well, Bluetooth is a very precise methodology to see down to a granular level where consumers are. But at the same time, we're seeing about 5% of the shoppers that walk into a store. So this is a technology that's suited to a very high traffic environment, stores that have 1,000 or 2,000 shoppers a day. When you're seeing 5%, it becomes meaningful data. And so that's really the way the approach is working.

And so if you're seeing 5%, maybe you're going to see a larger percent with Wi-Fi, maybe as much as 25%. But it's still a sample and it's not about trying to track or identify. It's really about creating insights that are useful to the business.

AMANDA KOULOUSIAS: Thank you. So we've gotten a lot of great questions from our audience. One of them that has come in is for Mallory. Somebody has asked if you could expand upon how this technology helps with loss prevention.

MALLORY DUNCAN: Sure. I mean, retailers use a lot of techniques for loss prevention. We have security cameras in the store, for example. We'll have anonymous security personnel in the store. It is also possible that if you see goods moving out of the store in conjunction with particular, again, anonymous identifiers, that shows you where there are leaks in your operation. And it can also potentially show you where there might be groups-- we have a lot of problems with organized retail threats-- there may be groups that are moving collectively in order to commit crimes in the store.

AMANDA KOULOUSIAS: Thank you. OK. And, Jim, one of these questions that has come in is actually about something you had said about the aggregate information. And so the question is, is the information aggregated at the retail location or is it collected and stored individually on your servers and then aggregated for reporting?

JAMES RIESENBACH: Well, let me try to interpret the question.

AMANDA KOULOUSIAS: Sure.

JAMES RIESENBACH: I assume that that's saying, how do we collect the data and report it? We collect everything specifically within each individual environment where we have presence. So for some chains where, let's say, we have 20 or 50 stores, each individual store is collected in its own data file, so to speak. And then what we'll do-- is it's important for our clients that they're able to see this data either at the store level, at the regional or divisional level, and at the corporate level. And so what we'll do is we'll-- in keeping with the notion of aggregated reporting-- we'll roll it up into the appropriate level of detail that the people that are going to actually use the data want to see it.

And in many cases, it is at a corporate level. But it's important for us that we're providing the tools. At the end of the day, if a retailer is trying to improve the customer experience, that happens where-- where the rubber meets the road is at the store level and the store manager really wants to be able understand what can they do on a day to day basis to staff appropriately, to market and merchandise their products appropriately, and to make sure that they have the right number of lanes and cash registers open.

KRISTEN ANDERSON: Thanks. At this time, since we talked a little bit about the insights that some of the retailers can gain and the benefits that can accrue to customers, we'd like to learn a little bit more about consumer's perspectives and their experiences, their navigating the retail environment. So at this time we'll invite Ilana Westerman to give a presentation on what she found through some of her research.

ILANA WESTERMAN: Magic? All right, thank you. Before I get started with what customers think and want, I want to just do a little bit of background. And, really, what we find is, is what retailers want to do is create trust with their consumers. And what consumers want is to trust the retailers. But there' four things that we really need to have for that to happen.

The first thing is that consumers have to understand, there has to be transparency. So they have to be aware of what's happening. The second thing is they have to have choice and they have to be able to control. If they care. They don't always care, but if they care.

The third is engagement. So if they do try to go control it, is it easy to do? And lastly, that they're getting value. So if they're giving you something, are they getting something back?

The other thing that I wanted to do just from a background perspective is talk a bit about design and how design differs from art. So if you're an artist, what you're doing is you're creating something for yourself. But if you're a designer, what we try to do is we create for the people. So it's really important for us to begin with, before we even draw anything, is to understand the people we're designing for. Who are they? What do they care about? What's their context? What's their environment? And making sure that we're designing for that.

So really what I'm going to talk about today is that first phase of understand and some of the research we recently did. So this is a fairly large study, over 4,600 Americans participated. We looked at retailers across the country-- they were only large retailers-- in a series of different techniques, both qualitative and quantitative.

And what we found overall is that Americans do trust. We do trust, in general, and we trust retailers a little bit more than average. It's a good spot to be in. The other thing we found is we're willing to give up our information. 97% of us will give up a piece of data for a deal. So it's not that we're not willing to do it.

So this short little video here, Alicia's going to tell us a little bit about what she thinks about an article she read. So this experiment, what we did is we had people read article about stores tracking their cells and asked people just to give us their reactions.

-I mean, that's crazy they can do that and the whole-- even if you don't sign into their Wi-Fi they can track you. But at the end of the article they talked about giving people the option to get Amazon credit or Google Play credit if they give their information and let people track them. Yeah. They will get a lot more people to agree to that, willingly than if they just took it.

ILANA WESTERMAN: So, again, as long as we get value we are willing to give up information. But what we find is people are much more likely-- 2 1/2% more likely-- to give up information if it makes sense to them. So here we asked people about giving up their location information to find something in the store. So a map type app. And it made sense to people why their location was needed. So 75% said they would give that information.

30% still would give information that didn't make sense-- the books and magazines that they read-- but still just to have an application like a map application, they would still give up that information. The other thing that we found, which is really important, is all data isn't different. Some data means more things to people than others. And the first thing is things that you would think-- like your name, your phone number, your address-- those are things to the far right, those directory information, people care the least about. They're very willing to give that information up.

But what we find people care most about is personal digital data. These are things on your device such as the pictures on your phone, your address book, your social network connections, those sorts of things people care the most about. And the reason we find that is because people say, these are other people, not just myself. I can give up my data, that's my choice. But I really don't have the right to give up somebody else's data. So my contact list has other people, photos of other people on my phone. So that's where people get really sensitive.

The other thing that's really, really important is a big distinction with location. So people are very willing to give up where their location is right now, they're starting to see benefits to that. It's not something they're terribly concerned about. But when you ask about where they have been, now people care and that's something that they don't want to give up. So it's a big distinction when it comes that type of location. So now, Mark also, in this experiment, read a similar article and he's going to tell a little bit about what he cares about and what doesn't matter as much.

-I could see why they would do it so that they know what customers are looking at at the malls or using their cells to gather information but that's kind of invading your privacy, though. I don't

mind if they're tracking what I'm doing in the store. But getting information in my cell phone, that worries me.

I wouldn't want them to get my contacts, my files, my apps, or anything from my cell phone. My location is fine. Where I'm walking through the store and then whatever cameras they're using tracking what I'm looking at and things like that, but my personal information, it bothers me a lot because I do have private information on my cell phone.

ILANA WESTERMAN: So what's really important as designers is to understand that because we want to message people and explain things to people who want to know what do they care most about. And messaging them about that versus things that they care less about. But the other thing that we found, which is really important, is that that component of trust that we really need before anything else is transparency. So people have to be aware that something's happening, otherwise they're not going to try and control it.

And so we this really low awareness overall of the fact that stores are collecting information. 33% think that maybe that could happen. It's a little bit higher when you ask only about location. But then we interview people afterwards, there's a lot of confusion around this. They say, well, maybe it could happen but I'm not quite sure how it would happen. And it's not very clear to consumers what's happening.

-So I said maybe just because this is kind of stuff that I'm unsure about. For example, one of my co-workers was just talking about something like this at work because we have Wi-Fi. And so, like, when you're at work or when you're in a store, whatever, it's all generally connected to the Wi-Fi and you might be looking at something on the internet while you're strolling through, you might be-- maybe you're at the register, you want to check your bank account real quick. Something like that.

But I don't know. So it's just kind of, like, a question that's been brought up so I'm not positive about. And I'm not really that good at technical things so I wouldn't really know unless I asked somebody who was. So that's why I was kind of like, maybe.

ILANA WESTERMAN: So from a design perspective we really want to start by creating that awareness. And so what we looked at is the most logical places are signage that's in stores or in device. And this would be an easy way to create awareness. So the first thing we did, we'd say, OK, let's look at signs. And so we had people go in to stores and shop for things and then we had them come back and draw out what they saw in the store.

And what we found is people only recalled 8% of the signs that they saw in the store. And so this is pretty low if you want to create general awareness. I'm going to skip this video. The other thing we found is that consumers-- when we have a consumer notification such as this one here that's in one of the counties where we did the research, 0% of the people recalled seeing the signs. And it was in all the stores.

And the next thing we want to look at is, OK, so fine. Maybe they can't recall exactly what they saw, but was there any form of ambient awareness. Did they see it out of the corner of their eye?

Where they aware that it was there and didn't actually maybe register specifically what the sign was? So we showed them signs that were present in the stores and signs that weren't.

What we found is, overall, people more often wrong than right. They thought a sign was in a store that wasn't versus a sign that actually was in the store. So there's so much coming at us, there's so much information across all these stores, all these signs, that we're not really paying attention in great detail.

-What I'm amazed at is how much I don't notice. That's amazing. I was surprised how much I didn't notice. I mean, you go to stores all the time and I guess you don't always notice. And they're spending all this money. I just thought, oh, my god, they spend all these monies for these signs and I didn't even notice them.

ILANA WESTERMAN: So why aren't people looking at signs? Well, we find that some people are in the mode of get in, get out. They really want to get that job done [INAUDIBLE] shopping. But other times when you're shopping you're really focusing on the product and that's what it's about, or the experience of the store. So that's where the attention goes.

But that doesn't mean there weren't some signs that did well. There are some signs that people did notice, that 8%. And what we found is there's three factors that really increased awareness.

The first is context. It's a sign that's part of the activity. So if you're trying to find socks in a store, the signs that tell you where menswear could be helpful. Also, when it's at eye level and there's a lot of repetition of the message then people recalled it. And, at a glance, easy to parse. So if you look at the sign over here to the right, all body care, that was a sign that was recognized by most people.

Compare that to the consumer notification sign with all those words, very hard to parse. So people aren't spending that time to actually engage with it.

So the next thing we wanted to look at is, well, can we just message on smartphones? And there was a good study that Google did recently that said 84% of smart phone shoppers used their phones in stores. And so what we wanted to try to find out is how often are they using the phones in stores. Because that could be another easy way to potentially message them.

But, unfortunately, what we found is that only 11% of consumers had phones visible at any point in time in the store. And so that's a pretty low percentage. We compared that to people who were in a mall area and we found that 30% of people had phones visible in that area.

And then we kind of looked at why. Why is this? Why aren't people having their phones out? Well, one reason is your hands are busy. And what we did then is we counted on people's ability to even have their phone out and available. And so what we saw-- we counted how many hands they had free. So whether you had no ability then, obviously, you couldn't hold your phone. You might have limited ability, have one hand free. Or you could have full ability with two hands free.

So in the stores, only 63% of people had some ability compared to 80% in the mall. So at the end of the day, if you ask us, should we not put notice on signs and devices? Well, it can definitely reinforce the message of what's being collected but it's not the way to really create widespread awareness. After people are aware, will they see it out of the corner of their eye? Yes, if the signs are well placed and the messaging is well placed and done in context it can. But at the onset, if people aren't aware, then this is not necessarily the way to create that widespread awareness.

So the next thing is-- this is kind of like a sad story. I'm telling you how everything doesn't work. Now I want to tell you how things maybe can work. So as designers we take that as, this is this context, we can't changes, we can't make people take their phones out if they don't want to, we can't make people pay attention to signs that they don't want to do. So, therefore, how can we solve this problem given that context?

So there's three different ways that you can really create awareness. The first way is the best way, which is called implicit awareness. And that is when you don't need notice at all. So an example is your map app. Does your map know where you are? Yeah. I hope it knows where I am. I want it to know where I am. I don't need notice to know that. It's implicit.

The second is explicit and that's direct communication. It could be an advertising campaign or something like just in time notice. And you have to get their attention for people to have explicit awareness. And last is that ambient awareness that we were just talking about with signs. And this is something that could be very helpful to reinforce what somebody already knows.

So just a quick hypothetical with implicit awareness. And this is how-- what we really advocate for as much as possible when collecting information is give people value that makes sense to them while you have it. So an example is, let's say you downloaded a wish list app at the holidays and all your friends and family join and told you what they wanted. And let's say that your mom really likes some perfume. I don't know about you guys, but I have a hard time buying for my mom. So she really likes a certain perfume and then when you walk into a retailer, it says, oh, yeah, we have that perfume.

So you go ahead and you buy it. And let's say next year you're online and you're at the same retailer site and they say, oh, by the way, if your mom liked that perfume, other people who bought that perfume liked this sweater. Maybe you want to buy her that sweater. And people love that. They're like, well, yeah, that would really make my life easier if I had that.

And all of sudden, what do I know? I believe that you know where I am, I believe that you know where I am over time, I believe that you know my social network, I believe that you know who I am when I'm on my computer or a another device and I'm getting value for all that and you haven't had to give me any notice. It's just implicit in the actual application. So Ellen is talking about this.

[AUDIO PLAYBACK]

-My niece wanted the Harry Potter movie and I walked into Target and they just didn't have. So it would've been nice is I didn't realize that I also went to Walmart that day, that I also was in

Walgreen's. If I was in that store and they alerted they had that movie it would have cut half time. So it would have been wonderful if I had a reminder of that.

[END AUDIO PLAYBACK

ILANA WESTERMAN: So the second thing is explicit awareness. And with this, we're really at this point in time where because people aren't aware we're going to use techniques around explicit awareness. And not everything can be implicit. There are going to be certain things that are going to be collected that people don't necessarily understand how it's actually helping them. So in these cases, the best way to do it is currently with just in time notice. So when you need information, asking for the information.

This crazy concept to the right, we're not advocating for but it's just a way, from a design perspective, you could solve it, which is potentially a way to plug in your phone and get power when you're in a store with a cart and then all of a sudden you could see your phone. So this is a way to overcome the issue of no hands. But this would be a potential way to give explicit awareness.

And then with ambient awareness, again, looking at the future, there's going to be-- as we see more and more wearables, the ability to do more tactile kinds of things-- vibration, things like that could come. But for today, right now, where we're at it's more about visual signs and screens. And, again, auditory might help in the future as well.

But this is a big design challenge. I mean, what we're trying to do is, people aren't aware of something and it doesn't always make sense to them why you need the information. So this isn't easy. This is something that's going to take time.

And so, what we've been working on first is a MyData symbol. So as we do explicit campaigns, as we do more around implicit awareness, at some point we have to continue to reinforce this. And we'd like this to be something that's really universal across all data collection. So the goal, really, here was to communicate to people that information is being collected and transmitted, we wanted to make sure it was flexible for all different types of screens and signage, and we're just aware that we're not going to get this immediate awareness.

So if you look at the image right there, the wheelchair image, that is a great icon, it's a classic icon. It tells you without any words what it means. That's very difficult to do. It's not something that's common in the icon world.

But when you look at the recycle icon below, that's also a very well done icon and it does explain what recycling is. But at the onset, it wasn't something that you could roll out without words. You had to explain it at first so that people recognize it and understood what it meant.

So it's a process. And we have tested over 300 symbols to date and we're still not there. So I'm just going to show you at a high level some of the things that we're looking at and what feedback we're getting from consumers. So these are just all the multiple different concepts we're looking

at, many of these tested fairly well. But over 300 different concepts we look at to even get to the point we're at right now.

And so what we did is we take this and we ask people, look at this and just tell us what you think it means. And we don't tell them anything about personal information or data tracking. And so we're seeing overall-- we give them a list. Some words actually do apply and some don't. And we're starting to see some traction here. We're getting up to 55% when it comes to sending and transmitting but MyData is still down at 32%. Not having people understand that this is MyData being transmitted is difficult.

When we compare it to a location symbol-- this is a positive control here- we're seeing over 70%. So that's really our goal. So we're going to continue to iterate and try to get there. But at the end of the day, this is the process I think we all have to go through from a design perspective. We're not going to, tomorrow, all of a sudden have people wake up and be aware. But if we can get to a point where we can actually create these implicit awareness applications, create an environment where people are getting value for giving their information, and then reinforcing in a way that they're aware it's happening and if they care about it, then they can go control it. If the don't care about it, it's not going in the way.

KRISTEN ANDERSON: Thank you, Ilana.

ILANA WESTERMAN: Thank you.

KRISTEN ANDERSON: OK. So we've been getting several questions from the audience and a lot of them have been about notice and awareness. Ilana talked a lot about that and how important transparency is. So we'll start off by directing questions to Mallory and just ask how you and your members have thought about providing notice and creating awareness around this type of mobile device tracking?

MALLORY DUNCAN: Sure. That's a very good question. And, as I said at the beginning, it's really about what is necessary in order to preserve the level of trust with your customer. Let me give you one easy example I think will make it clear. There's a lot of discussion in this field about talking about tracking. One could just as easily, in many cases, substitute the word observing and it suddenly sounds a lot less scary. And the question is, do you have to give notice for observations?

One example, in the retail environment, would be the use of heat maps. Both the gentlemen here provide heat maps that show how groups of people move around the store. Well, you could have a situation, say, in a grocery store where, when most of us shop, we go off first immediately to the produce and we end up buying the frozen food at the end of the transaction.

Well, if you've got heat map observation of the flows in your store, and you see an unusually large number of people in the frozen food section, it means they're probably about to check out. So the retailer might take that information and say, OK, I'm going to open up more lanes, get more sales associates up front so the amount of time it takes people to check out is a lot shorter than it would be otherwise. Now that, I would argue, is a benefit to consumers. But it's not

necessarily something that you're going to provide notice about because it's almost an intrinsically good management of the store operation, as I was talking about earlier.

Now, why is that important? There's obviously a big conflict going on right now, or at least an apparent conflict, between online stores and brick and mortar stores. One of the things customers like in the online world is that they can very quickly accomplish their shopping and many online stores have moved to one click shopping, one quick check out. So, in the brick and mortar environment, if we're going to compete in that area, those stores would like to replicate that very fast click through check out which means putting more sales associates on the line, getting customers out of there so that in the brick and mortar environment you have both the personal interaction of being able to get questions answered quickly and combine that with a quick check out, which lets the brick and mortar stores compete more effectively with the online store. Again, all of this is part of competition, all of this goes to building consumer trust, none of it requires notice.

JAMES RIESENBACH: Mallory, can I ask you to follow up on that?

MALLORY DUNCAN: Sure.

JAMES RIESENBACH: So one of the things that we've come to understand is that consumers basically understand when they enter a retail environment that there's been loss prevention surveillance techniques that have been used for years and we've come to believe that that's a common awareness and understanding among consumers when they enter most retail environments that that's part of the approach that retailers are taking and not to mention that once they do check out and actually buy something, all of that data is part of the record permanently as well. So do you think that there's already a high degree of awareness among consumers about these types of things?

MALLORY DUNCAN: I can't say what the awareness is to any specific element that you mentioned, and that will vary from retailer to retailer which is what makes competition and what makes it possible for retailers to garner trust with their particular set of customers. But by and large, the fact that you are engaging in observable activities in a store is something that people are aware of.

Now, in terms of the details of a transaction, that will vary dramatically from one retailer to the other. In some it's essentially an anonymous transaction. In others, if you've opted in to a loyalty program, it may be much more detailed. So it's varies tremendously.

KRISTEN ANDERSON: Is there something unique about this type of tracking, though, that does require notice? And, Seth, you may have something to say about this and we'll follow up with Glenn and Jim as well.

SETH SCHOEN: I mean, I feel like hearing all of this I have quite a different paradigm because there's been a lot of focus in this conversation on notice and not a focus on consent and not a focus on whether there is an underlying hardware problem with the possibility of tracking occurring without people asking for it. And so, I would start much earlier in the process and

rather than criticize people on this panel I would criticize the IEEE 802.11 standards committee and say, why did you put a persistent unique identifier into people's phones? Why didn't you recognize people's privacy and security interests in not having something in their pocket shouting where they are to everyone who sets up a laptop to look at them?

Now, there is this conversation that we've been having and hearing here about, well, if a retailer puts this up for a particular purpose then there's a question of how appropriate is their purpose or how invasive is that or is statistical information is not very invasive at all compared to profiling? But I would start earlier and say, why are these devices screaming an identifier to all and sundry in the RF environment and saying, hey, it's Ashkan's phone, hey, it's Ashkan's phone, hey, it's Ashkan's phone?

Why did the standards committees make these identifiers unchanging and persistent? That's really where I would start. Now, I think there's a lot of merit in saying-- well, in the context of a particular retail use, it's not necessarily what people are expecting, it's not necessarily something that they've consented to. If you ask them in a survey, they wouldn't necessarily know that it was happening or that it was physically possible or how it was done. But, for certain categories of use, there's not necessarily a lot of harm, in that instance. And there may be benefit in that instance.

So from the perspective of the individual retailer, or from the perspective of the individual retail industry or from the perspective of the folks on this panel who are doing these analytics for statistical purposes, they can say, well, given that the technology is there and given that this is possible and given that we're trying to do this in a relatively noninvasive way for relatively noninvasive purposes, you shouldn't blame us. So I'm going to provisionally grant that and say, let's blame the technology industry for putting these persistent unique identifiers that can be read without consent by strangers wirelessly without people's awareness in any situation for any purpose into things that people are carrying around all day in their pockets.

KRISTEN ANDERSON: Great. Thank you. And so, Glenn and Jim, I think one of the things we wanted to hear a little bit about is your company's thoughts on are there ways that your companies are working to create transparency around the use of this information?

GLENN TINLEY: I want to answer that but I just want to also just make a clear distinction that-- and there's a lot of conversation and there's actually a lot of market confusion. I spend a lot of my time speaking with clients and potential clients about the confusion that is-- there's applications that are on a device that a person downloads and, as part of that, accepts certain terms and conditions that we all understand, that 99.9% of people are not reading. But those are accepted and it's those applications that are-- and Ashkan's presentation demonstrated it-- that the Pandora app is streaming information about the device or the person and different things on those devices to two different parties.

And in the other presentation, one of the videos was, you know, I have personal photos on my phone and I don't think those should be shared. And we agree 100%. There's a difference between monitoring, observing, tracking, of something from an application that is on a device that you are using versus a device being seen or observed as a dot.

And the analogy I would give to our clients is, think of it as I have a bag of beans and I'm going to make soup, and I pour all the beans into the soup and I stir it all up. Go and tell me where-- I put them into different bowls, but you don't know which bean came from what and we don't really care. What we care about is the fact that these beans are in here and we know that there's some over here and there's some over here and some never actually got out of the pot. But we're not necessarily concerned about what bean is what and who we're going to associate that with.

We're not interested in individual consumers and there is no technological way to take a Mac address and determine or go into a device. There's no connection ever made to a device. So an application, there's a connection made to a device and that connection made to the device allows it to obtain information. We don't do that in any way, shape or form.

A phone calls out, a mobile device calls out and says, to Seth's point, yes, I'm here. We see a number, sort of like a vehicle identification number on a car-- it's unique to the car, it's unique to the device-- but that's all we know. We just know that it's a car. We might know it's a Ford car and we might know that it's an iPhone. But that's it. We don't know that it's Ashkan's phone.

And so there needs to be a distinction that we are not tracking or monitoring, observing any of that application data. We're taking the data that is completely almost irrelevant because it can't be-- there's no connection made to a device to go and capture any individual information at all or see what you're looking at or any payload data or anything along those lines. So there needs to be that that distinction in that regards.

And then, again, to Mallory's point, that there's a large amount of trust that retailers have with their clients inherently, or the customers inherently. Retailers want to understand what's happening so that they can help make the customer experience better. They're not interested in any way, shape or form of upsetting the apple cart of the trust that they've spent years building with consumers to make them loyal customers. A retailer would never then take that and say, well, now let's start to try to identify-- without people knowing, let's try to identify who these people are so that we can do something that's going to degrade that level of trust that we've spent years building.

So it's not application based and it's completely separate of that and completely not connected to it at all. There's never a connection made to a mobile device at all by anybody in the industry. And then secondly, that inherently there's that level of trust that retailers are adamant about protecting and they want to make sure that that's being protected. So those are the-- they're not going to do something that's going to upset that. So I hope I answered the question, Kristen. I probably got off track.

JAMES RIESENBACH: Let me add to what Glenn was saying. I agree with his points but I do think there was a question about what are the company's doing specifically to help with disclosure and awareness. And we as an industry, and Glenn's company, my company, and a dozen others have been participating in what we call a code of conduct across the industry that essentially establishes guidelines. And, in many cases, there's aspects of this that we have agreed are legally binding on the companies that are involved.

But there's a set of principles that we went to develop this under, recognizing that this is an evolving marketplace and technology is evolving quickly. So we can't let good be the enemy of perfect or vice versa. It's important that we know that this is one step in a continuously evolving process.

But what the core principles are, first of all, is that we will do everything we can to create that level of transparency and disclosure. And so what we are doing is we're asking all of the-- every firm that participates in this code is asking the retailers to provide signage. Now, what are we doing? I think to Ilana's point that awareness is relatively low of signage, well, we believe the best thing to do is to come together as an industry and we're working with Ilana and trying to create some types of visual cues the will have that type of ubiquity when they're out throughout the marketplace and over time.

We don't believe today a consumers going to walk into a store and know what that means. But we do believe that when that's spread across tens of thousands of stores across the entire US, and consumers see it on a daily basis, that it will become a visual cue the will tell people what's going on. And so that's a step along the way from a disclosure standpoint.

We're also putting it on our websites, we're asking our retail partners to put it on their websites, what we're doing. So we're doing the best given the current methodologies available to us to disclose as an industry.

The second is that we're providing choice to the consumer. And what's really important is that if a consumer does not want their device to be seen, even though we're only aggregating and providing statistical insights, that consumer has an ability, as of now, to opt out. And not only to opt out with our company or a particular retailer, but to be able to opt out of having their device seen across the industry. And so we announced yesterday with our group, in addition to the code, that we have launched an opt out capability.

And we've done this in conjunction with a company called The Wireless Registry. They've created the code. And essentially what we're doing is allowing consumers to opt out across the industry. That will be active within 30 days. So we will allow consumers to opt out.

We have a variety of other aspects of the code. Some about hashing and preventing us from, basically, collecting the actual Mac addresses and storing those. So we all agree that we will hash. I understand Ashkan's point that it's not impossible for that to be used in other ways, but for all practical purposes, we don't believe that that is a reality any time in the foreseeable future. For right now, what's important is that we move forward with that.

And I think that it's also important that we hold not only ourselves but our clients accountable to the use of the data so that we have within the code an understanding that the data will not be redistributed to someone else or aggregated with other sources of information that could be used to personally identify the individual. So we're trying, as an industry, to be good actors. We're disclosing this, we're doing everything we can to communicate this across the industry right now.

ILANA WESTERMAN: And I'd just like to jump in here because I got really concerned when you mentioned that this is a bad thing, that you're having your address put out there. I think from a consumer's perspective there's a lot of value they can get. I mean, being able to walk into a store and have it know you and know what you like and recommend things to you, there could be a real benefit to this.

SETH SCHOEN: You should install an app for that store and say, when I go to this store I want you to tell the store rather than have your phone do that for you without consent for every kind of entity that could possibly be listening.

ILANA WESTERMAN: There could be ways of going about it but to shut down the ability to innovate, the ability to personally identify each person, potentially, and be able to deliver value to me that I want in the future, that might be beneficial to consumers. They might like that. And so, yes, having that transparency, making sure they're aware is important. Having that control is very important.

But at the end of the day, do retailers really want their customers to be angry with them? I just don't think so. I think they're trying to derive more benefit and I'd hate to see that shut down. It has to be done in a way that creates trust. There are good ways to do it and bad ways to do it. But to shut it down, I would be concerned about.

SETH SCHOEN: So I think it would be a lot of fun to talk about hashing and it may be kind of a distraction from the more fundamental privacy issues. But I just wanted to say, hashing doesn't work for the purpose of actually making yourself not know a Mac address or actually making yourself unable to recognize a Mac address or get the history of it. And the blog post by Ed Felton that Ashkan pointed to goes into this a bit. The problem is that the space of possible Mac addresses is too small, and as Ashkan alluded to, you could actually try every Mac address as a candidate and put it to the hash and see if it's that one.

So I actually want to issue a challenge to the industry if people think that Mac addresses are somehow not readily identifiable. I want you to send me a couple of hashed Mac addresses that you've actually collected in the wild of actual mobile devices, tell me what the hashing algorithm was, and I'll crack them and tell you what the Mac addresses were. I don't think it's technically challenging to do so. The space of Mac addresses is just too small to make that actually difficult to crack.

JAMES RIESENBACH: And if that was done, what would be the use of the Mac address? Because that still doesn't encompass any personally identifiable information. It would be something that's identifiable to a device. So, as I said, we try to look at this through the filter of practicality and is there some use that could actually be meaningfully harmful to consumers if even you were able to go through this process and take the time and cost and resources to actually go and find a Mac address?

SETH SCHOEN: I mean, I think the time and cost and resources is about a week of time on one laptop. And I hope that people will take me up on this challenge because I'm actually do it and

show that it's a real possibility. And it's not like I'm going to rent a supercomputer. It's like, I'm going to run it on my laptop and brute force it on one device. That's my expectation.

I think that a lot of people have said that any given identifier is anonymous in some sense because it doesn't have someone's name on it. And actually, Latanya Sweeney was a pioneer in questioning that and there's been a whole academic field within computer science talking about deanonymization of data. So people have certain intuitions about something being anonymous and you're starting from a certain point and you're saying, well, that's not someone's name, so I don't know who that is.

One of the underlying difficulties is that you have something that, although it's not someone's name, is unique. And it's unique in all the world as a Mac address is. And so if you have some circumstance where you have some opportunity to observe that thing, or some database that contains that thing along with other data, then that can be combined. And we like to say that deanonymization is really a one way street. You can go down the deanonymization street and then the anonymity has been lost.

So I know that with this code of conduct the part of the industry that's represented here is very solicitous about the idea that they don't actually want to know who you are and they're not actually going to make efforts to know who you are. I think Ashkan's presentation, referring to the CVS app, pointed to the fact that there are a lot of pressures to do that and there are a lot of companies that will be interested in doing that. And they may not even be companies that see themselves as part of this particular analytics industry or that see the code of conduct as even relevant to them.

But Ashkan has already demonstrated on his slide that there are companies that are collecting Mac addresses from within apps. And those companies absolutely will know the identity, in the classic sense, of the person to whom that Mac address relates. And they're making those associations because they're interested for their commercial reasons or whatever reasons. And those associations, technically, are very easy for app developers to make if they're interested in doing it.

So there's a prospect, and it's not a prospect, again, that these companies on this panel are interested in doing for their business purposes, but it's a prospect that other parts of the industry will be interested in, I think, which is converging different kinds of analytics and converging different kinds of data sets and saying, well, if we had the ability to know you're offline identity and your online identity and how those relate, why wouldn't we do that? And, again, these people on the panel have businesses that don't rely on that and they don't do that and I think that's great. But I think that there are other parts of the industry that say, well, if we have that capability to make those associations, why not?

ILANA WESTERMAN: Well, I guess I get concerned, too, when I think about the potential for data and collection and analytics being good or bad. Data, in and of itself, isn't good or bad. Analytics isn't good or bad. It can be how it's used.

And we did an interesting study recently where we asked people, let's say a child's tracked from five years old on. Everything ready for school was put out there and analyzed. And let's say there was algorithms that were written-- and this hypothetical-- to figure out that kids who spelled poorly and liked the hamster dance on YouTube would do better at UCLA versus University of Michigan. So let's say this happened.

When we asked parents and say, and let's say you could have that information to figure out which school your kid should apply to. People loved the idea. When we asked the same question, well, what if the schools used that to admit students? People hated the idea.

So the concept of the data itself being collected is bad, the algorithm is bad. To me it just concerns me that we're limiting ourselves in the future for what could be innovation. There's definitely boundaries. People care, right? And we have to make sure we understand those and understand that context and decide within it. But just to shut it off completely and we shouldn't be doing this and everyone always wants to be anonymous, really limits the future of potentially getting more value to people. So it just concerns us.

SETH SCHOEN: Well, the process of community, I think, really has a consent model where the distinction is consent and the default for the privacy community is that people don't know sensitive personal information about you unless you decide to share it with them for purposes that you understand. And I think that's a good norm and that's an appropriate norm and it's not a norm that very many areas of technology are respecting today. Whether this area of technology or others.

JAMES RIESENBACH: However, but--

ILANA WESTERMAN: People want choice, you're right. Consent needs to be there. Sorry.

JAMES RIESENBACH: Go on.

ILANA WESTERMAN: So you have to make your consumers aware. You need that transparency. They don't like to be surprised. They want to know what's happening. And they do want to have choice if they care. But I think the idea that everybody wants to be anonymous and nothing should be collected-- that's my concern. We might limit ourselves for future value.

SETH SCHOEN: If you have someone who realizes someday that they didn't want something to be known from, say, a year ago, that they didn't even realize technologically could be known, it's a bit late for them to go back and erase that data which is considered the property of the person who observed it, typically. It's a bit late for them to go back and say, oh, I didn't know that you could know that about me, about what I did a year ago, about who I was with, where I was with, what I was doing. Now I regret it now that I know and I want you to erase it. Well, it's a little late for that.

AMANDA KOULOUSIAS: Great. Thank you. So I think everybody has made some great points about some of the differences if this information which become identifiable or whether it may become identifiable. But we want to take a step back for a minute and talk about what's going on,

mainly right now, which seems to be the aggregated analytics and transparency around that. And so what we want to kind out, are stores that are using that-- the aggregated analytics-- notifying their customers right now?

GLENN TINLEY: Well, with our clients, as part of the code of conduct, they're incorporating it into signage within stores. And they're doing that in different ways. Either existing signage that is being redone with information being put in or in other ways that-- customer service. We've had conversations with store managers that if there's a question that comes up, we're helping them to make sure that they can address and answer those questions as well.

It's not a-- there is transparency. They do want consumers to understand and realize, but there's, again, the diversion of the-- you're collecting something personal about me just because you see my Mac address or can-- you can't send an offer to a device just because you have a Mac address. You have to have something else to deliver that. And that needs to mean that they opted into it. So they're cognizant of that.

But, yeah, they are looking at signage and putting up signage. And we're recommending different signage where there's a smart store privacy or a smart store logo. There's different things. And Ilana's working on things to help move that along so that more and more that's being adopted.

MALLORY DUNCAN: I have to step in here because although I appreciate the debate about the signage or the approach and the various elements that might go into this proposed code, on behalf of the retail industry, I have to say that the overwhelming majority of the industry is not at a point that we think this code has all the elements that we think are necessary or appropriate.

Just using the example I gave earlier in terms of heat mapping for purposes of shortening checkout lines, it's not something that we think is necessary to be oversigning in stores, especially if we have evidence indicating that most consumers aren't reading most signs anyway to suddenly proliferate whole bunches of new signs either for this technology or for other technology that's used to accomplish, essentially, the same thing. Strikes us as perhaps a bridge too far at this point in light of what's actually happening.

JAMES RIESENBACH: There's certainly an issue where it's early in this game, it's constantly evolving, and the approach that we've taken within the industry is, as I said earlier, we're not going to sit here today and say this code or what we're doing is the perfect solution. But we felt that there's a lot of confusion out in the marketplace and this is a good first step. And the retailers that we're working with-- and I've heard that from others in the industry as well-- are asking for ways to inform not only their consumers but even their employees so their employees are aware of what they're doing.

So we recognize that this is not the ideal perfect solution forever and that there may be, to Mallory's point, many ways that we should be doing it in a much broader sense in conjunction with all possible technologies and conjunction with all retailers. But that's something that, for practical purposes, we could probably be talking about five years from today. So our attitude has been let's get as far as we can right now, let's get something out into the marketplace that shows

positive intent, positive steps, and what we can do today as an industry. So that's been the approach.

ILANA WESTERMAN: And I would say the best way we see is that implicit awareness. And if we can do more of that, creating that value for consumers-- so I have an app, for example, that knows where I'm at and gives me a value for it-- then all of a sudden, if you use that information to do heat maps and make the lines shorter, people are very happy about that. That's fine. They're aware that you have the information and you're using it for good.

I think trying to get people to stop and pay attention to things is always going to be difficult, especially when there's so much going on in a retail space. But I think there could be a win-win here, is that the more functionality comes online that uses this information that helps consumers, then you've created awareness without the notice and you've created an environment that helps the retailers and the consumers.

And then what happens is you get the ambient awareness of the notice that's there so people, if it's placed properly, once they're aware that it's happening, if they care, then they become aware that, OK, here's a store, maybe I don't want it to have it and then I can opt out. But in general, I think the implicit awareness is the right first step to take.

KRISTEN ANDERSON: So my understanding from Jim and Glenn was that you are already taking steps to make explicit the notices in your current locations. So with your retailers, Jim, are they-- they're putting up physical signage in the stores? Are they putting them at the registers, are they putting them in the windows? And then, Glenn, for you I think you were saying that a lot of your clients are bigger clients like shopping malls and airports, so do you have an example of where that signage might be and how consumers might notice it.

JAMES RIESENBACH: Well, we are working with retailers. Knowing that we as an industry are working to develop a set of signage and visual cues that we're going to carry across all retailers and across all of these companies, we've been working on an interim basis to put some signage up but we have also, essentially, informed our retail partners that we are working on something that we will be delivering. And that's something that's part of the coalition that we've put together and working with Ilana to develop. So we're expecting that it's going to become much more prevalent as we get through this year.

GLENN TINLEY: And we are much the same but we've got some of our clients that-- they have existing signage on the wall that will talk about different privacy policies or different codes of conduct that the mall owner or operator will abide by in different wings of a mall. And it's being added-- in most cases, it's being added as one of those items in there.

KRISTEN ANDERSON: Thanks.

AMANDA KOULOUSIAS: And so we've talked a little bit about whether notices are being provided and where they might be being provided. And so the question that I wanted to raise for everybody is, what are the goals of the notice? What are the important pieces of information that need to be conveyed to consumers?

ILANA WESTERMAN: Well, what consumers care about is what information is being collected and how is this being used. And so if you're asking somebody to make a choice about something, they need to understand the implications. As you saw in some of the videos, frequently it's something that they don't care so much about it or if it's being used to streamline things they're OK with it. There's other things they care a lot more about. So if those things were being collected, we would be much more strongly advocating for different types of explicit awareness type notice.

But one thing I would like to bring up is the mall areas. And that's something we didn't research so it would be the next step. Since we're seeing many more phones out in the mall areas, we're seeing people having more attention paid in the mall areas, that might actually be a place where you could get more awareness of signage. I don't have the data right now so I don't know, but that would be a next step to look at. Is that a place that we could place them?

JAMES RIESENBACH: The other thing is that there are ways, and we're experimenting with this, that the signage can actually convey a consumer benefit. And so one instance where we're doing this right now is in airports where the TSA queues can back up and you can have hundreds of people in line, but there could be three different TSA queues at the same airport. So what we're doing and, as I said, we're testing this in a number of cases, is we're using our methodology to put big monitors up at the beginning of each of the TSA queues to tell the consumer when they get there what's the wait time in this line.

It says, line one, 12 minutes, but line two is eight minutes and line three is four minutes. So it is a self regulating path for consumers to actually benefit and see how they can save time at an airport. and we're using this same approach in many cases. And, as I mentioned earlier, in grocery stores that can be a very similar approach. So there are some direct consumer benefits that tie into the signage and the disclosure.

AMANDA KOULOUSIAS: Thanks. And so one of the things that you mentioned before is that with this code of conduct that consumers have the ability to opt out. And so is that ability to opt out something that is mentioned in any of the notices that are being put in stores.

GLENN TINLEY: Yes. As part of the signage or verbiage that's being put up, there's a website address in most cases, or in all cases right now, to be able to go and do that. And as Ashkan pointed out, and as I think we all understand, that is not the most seamless, or it's not the seamless way to be able to do it, but it is a way to do it that does give consumers the option to do so.

We've also had emails from people who have just said, here's-- I've seen a sign and here's an email and can you please remove me. And we do so and we respond to the email immediately to say that this has been done. So there are ways to do it and there is a web address or something being applied in there.

JAMES RIESENBACH: I think we've all learned, and Ilana may testify, that as soon as you start to try to convey too many messages with too much information in too many words on a sign, you essentially lose the chance of actually communicating effectively. So what we're trying to do is

minimize the amount of text, maximize the amount of visual impact as well as giving a very easy way for consumers to know where to go to find that information.

KRISTEN ANDERSON: We've gotten a lot of questions about where people can find the code online. I don't know if any of you has a URL with you that we can provide but we would like to be able to do that. And then also, if one of you can talk a little bit more about how the opt out actually works, how consumers access it. Once they get to the website, what do they have to do?

JAMES RIESENBACH: We're working with an organization called The Future of Privacy. They're a Washington based think tank and they've helped us to put this group together and develop the code. And the code is actually live on their site. Now, all of the companies that are participating are also putting this live on our sites as well. And then, of course, within the opt out there's going to be the information when people go into that. If they choose to opt out there's much more information, there's a whole frequently asked questions area that talks about the code.

KRISTEN ANDERSON: Instructing you on how to find your Mac address and enter it and all of that? OK.

AMANDA KOULOUSIAS: Seth, so we wanted to go back to you on some of the points you had actually made a little bit earlier, some of the concerns that you had about persistent identifiers and how they're being broadcast from the phones. And what I'm wondering is, given the fact that the Mac address is being broadcast from the phone right now- that is what's going on--- what are your thoughts on transparency and choices for consumers around that and why it's needed and ways to do that?

SETH SCHOEN: I mean, I think that the people who are making these devices, in a sense, are, as I phrased it earlier, more to blame for the prospect of people randomly knowing where you are at any given moment and situation and place. I guess I'd like to see device makers warning people, when you use Wi-Fi or when you have Wi-Fi on, the Wi-Fi networks that you're on or near can recognize you.

I agree that there's a very challenging question about how to convey information and how to get people to pay attention to it, whether they're in a store or whether they're opening their cell phone for the first time. And I don't presume to know the best way to go about conveying that but I'd like to see device makers actually warning people, people will know where this device is when you use it as intended. And these are some of the kinds of people who can know that. So that's something that I'd like to see. I certainly think that if there's a store or somewhere that's doing this, that putting up a sign, as we've just been talking about, is an appropriate thing to do in that context, that it's a sensible thing to warn people and to give people an opt out.

I guess, as I said earlier, thinking of the app that Ashkan found that's collecting Mac addresses, I'm much less concerned about the relatively responsible people who are affirmatively interested in warning people and in giving people an opt out and in giving people more control, and I'm more concerned about the notion that there's really such a low barrier to entry for location tracking. For those of you who were here in time to see the demo earlier, that demo of location

tracking was done on an ordinary laptop with very ordinary hardware. It wasn't done with some super high tech thing that's only available from government research labs or something. It's an ordinary laptop.

And in fact, Dr. Sweeney was saying that she had to actively program it not to track everyone who walked by, and that was an actual effort that she had to go to make sure that it wouldn't track all of you as you walked into the building. So the barrier to entry for doing fairly involved tracking is relatively low and there are a lot of different kinds of entities that could undertake it, not just entities that have signed on to the code or that are trying to put up signs and inform people.

MALLORY DUNCAN: May I just add on to what Seth was saying here. Look, this is relatively new technology. There are some advantages to the retailers and to our customers from its use. But it's not so pervasive that it is critical to retailer's operations. We would like to see it grow and we're not interested in seeing technology arrested, I agree with Ilana on that. However, if device manufacturers wanted to put a kill button on cell phones, that would be something that you wouldn't find the retail industry objecting to as a general proposition.

SETH SCHOEN: I think them the more concretely useful thing would be a button that says, Change My Mac Address. And I don't think that-- I think it has substantial privacy benefits and I think it has very few adverse technical consequences. And I think for the statistical purposes, at least in terms of dwell time, wait time, not necessarily in terms of repeat visits, you would still be able to do that. So certainly if we're thinking about what button we'd like to have, I'd like to see the Change My Mac Address button. Now, it does mean that you wouldn't get the repeat visits or the repeat visits data would be a little bit less accurate, but for the dwell time and wait time you could still get that.

GLENN TINLEY: Seth, I also just wanted to bring up a point then that goes back to the CVS app is, within an app, when an app is downloaded-- and Apple did this and Google is actually doing it with their new versions of Android-- the Mac address is actually wiped out. So there is actually no Mac address broadcast when you're in the Google or Apple, I call it their ecosystem. The Mac address is actually not translated. It's a zero, two, and a series of zeros. Apple and Google apply an identifier, unique identifier, to the application or to the device.

So then, because Jim and myself and others, we live outside of that ecosystem and we see that Mac address, we can't actually-- we could not even then combine, even if technologically we wanted to, we could not combine the application that someone has and a Mac address to the generic Mac address or the Mac address that we're capturing. There's no way for us to even combine those. So, again, it even, from our standpoint, separates the ability to collect anything personally identifiable or anything along those lines. It puts another-- we call it a wedge-- in there as a protection against that and against profiling and their sort of negative connotations of those things.

SETH SCHOEN: So I think it's very important that mobile operating system developers should prevent applications from reading the Mac address as well as other identifiers.

GLENN TINLEY: Apple and Google do that.

SETH SCHOEN: And so there is a trend in that direction in recent mobile OS versions and I think that's great. And I think that's very welcome. I think a bigger picture indication from what Ashkan found is that there were app developers who were willing to try to use that information if they had access to it. And it suggests to me that whoever created that app is willing to try to use other technical means to circumvent that privacy measure.

And my prediction is that there are other technical means that are available. We can talk about-- I think it should be a separate conversation later. I think there are other technical means that will be found to circumvent that privacy measure and do that reconnection of MAC address and identity. So it's not necessarily that it's going to be the particular way that Ashkan found that the CVS is doing it. Which I agree [INAUDIBLE] OS developers are trying to plug that hole. It's that there is the willingness in some parts of the industry to try to make these associations. And I think that we're going to see that technologically, in this context, where there's a will, there's a way.

ILANA WESTERMAN: One thing that I'm also kind of concerned about is that we're oversimplifying the problem. And so when you talk to people about anonymity, there are definitely when we want to be anonymous. But there's also times when we're OK with you kind of knowing who we are in aggregate. And there's also times that we actually want you to personally know who we are.

So an example this is like when you're checking out at a store and you don't want your credit card taken, do you want to personally be identified? Yeah. People don't sign the back of their credit cards. They want you to look at their ID.

There are times when we really do you want that to be in place, and there's other times that we want to be anonymous. I think that it's a difficult design problem. We have to take a step back and look at what consumers really want, what do they really care about, and not oversimplify the solution and not assume it's going to happen over night either. All working towards that positive outcome, but we have to first deeply understand what people care about.

AMANDA KOULOUSIAS: I just wanted to follow up quickly on a point that you had made when you were talking about the ability to possibly reset a Mac address, one of the things that might be lost was kind of the new verses returning visitors. And so what I wanted to just hear briefly about is, to what extent do you think the privacy concerns differ if you're looking just at the current location versus that location over time with the returning visitors?

SETH SCHOEN: I think location over time-- Ilana alluded to the idea that it's something that people are anxious about. And I think people have very imperfect memories and machines have perfect memories, and people often don't even remember the sensitivity or the potential sensitivity in things that they've done and the places that they've been. An amazing example that someone working in this field gave me a few years ago is that you can use location to detect if people are having an extramarital affair because certain people spent the night in the same place.

You observe them in the place in the evening and you observe them in a place in the morning. And that sort of falls out of location accidentally.

Obviously, no one has started a company to detect if people are having extramarital affairs using location data. But people's sort of imperfect memories make them not even see the sensitivity in the location trail that they leave behind and the data trail that they leave behind. And for that reason, Bruce Schneier has compared data trails to a kind of pollution because you can't necessarily see it and you're not necessarily harmed by it in the short term.

So I think the inferences that are sensitive, that can be drawn from people's locations, clearly are much more extreme over the long term in terms of people's habits and habitual activity. And someone goes to a particular places of worship every week and you conclude that they probably are a member there and they probably actually belong to a particular religious group, as opposed to someone was once observed apparently at that place of worship. Well, maybe they were attending a musical concert or something.

So all of these things, as you get the overall picture of someone's life, of someone's habits, of someone's associations, are much more significant over time. And I agree that there's not that much sensitivity in a momentary observation. Oh, this person went to this store on this one day. That's not really very sensitive at all. But, oh, this person goes to this kind of place. Oh, this person knows this person because they were seen together. Oh, this person is in an intimate relationship with this person because they were seen together in certain kinds of places. That's much more sensitive and that's information falls out over time.

AMANDA KOULOUSIAS: Great.

GLENN TINLEY: Seth, just also-- just wanted to follow up on that the inference is that if you were sitting at our company, we would have to have our sensors installed at all of the hotels, every place of worship. We would have to have-- we would be everywhere. Which I'm wonderful to have that happen from a business standpoint, but the reality of it happening is we're sort of-- we're reaching a little bit in terms of the place of worship would have then hired us to install our sensors within there to then observe their visitors every Sunday to find out who's coming every Sunday or how many-- what percentage of them are coming every Sunday.

If they were then to use that, they wouldn't-- it's their data to use. They wouldn't use that to then profile their own people. So it's just-- and this is where sometimes it gets-- you can go a little-- we can get where there's so much data being collected and there is a lot of data being collected, and, obviously, protection of that data is paramount. But there is things required to have connections drawn and in almost all cases those things that are used to connect those things are not connected at all. And never could be or never will be.

SETH SCHOEN: So I would absolutely agree that the current scale of commercial location analytics is not dense enough to make some of the most extreme privacy invasive inferences because you don't have sensors in a lot of the places that people are most anxious about people knowing that they've been. And you may never have sensors in those places. I guess it's a big

picture concern and it's a long term concern about as you get more uses of location by more kinds of entities, some of those things actually will show up in some of those sensor networks.

And in the online world those are already showing up in the sense that websites are able to get that from IP address. And as I was discussing with Ashkan, there are companies that are trying to bridge the IP address and physical location world. So if you look at the big picture of the industry, I think some of those concerns can develop over time.

AMANDA KOULOUSIAS: Thanks. We really hate to cut off the conversation, but we are basically out of time. We want to give everybody just 15 seconds each to kind of give your closing thoughts on this. So we can start down at the end with Glenn.

GLENN TINLEY: Again, just to reiterate that we agree and support 100% that consumer privacy is, again, paramount to everything that is being done. I think that, as an industry, we actually stepped up and said, look, we understand this and we want to develop a code of conduct that is at least a starting point that can help bridge some of the next time frame. My only caution is the market confusion over what is within an app that somebody is downloading and using on a daily basis if they want to use that is not even giving out a Mac address versus what is being observed on an ongoing basis to help retailers with customer experience and just compete in that more online world.

MALLORY DUNCAN: I think I'll conclude as I began by saying that this ultimately, at least in the retail environment, is going to come down to a matter of trust. Rather than talking about notice for observations, we should be talking about notice for particularized uses that might be problematic. And that whether a use is problematic will depend upon the relationship of the customer with the environment they're in. In the store environment, for the reasons I said before, it's likely that the store is going to find-- try very hard to find that right balance. In a more open environment, say in a mall where the customer doesn't have a relationship, or perhaps in an airport, there may be a different paradigm applies. But at least, from our perspective, trust is the key.

SETH SCHOEN: So I'd just like to remind everyone again that Dr. Sweeney set up that demonstration on an ordinary laptop and had to actively program it not to collect all of your Mac addresses. And if she hadn't actively programmed it that way, then all of your devices that have Wi-Fi interfaces enabled would have an observation in that laptop saying that you were here at this time. And maybe it's not very sensitive to hear that you were here at this workshop at this time, but maybe there is some place or some interaction or some relationship that you wouldn't actually like someone to be able to observe in that way.

And so I think these statistical and aggregate applications of location analytics are not the scariest ones from a privacy point of view. Obviously, the profiling analytics that we haven't seen deployed commercially so much to date are dramatically scarier. But I think the barriers to entry are really extremely low and I think, to the extent that people want their location to be used to provide services to them. and they want people to know their location, it is very technically easy to do that in a consensual way by having people install applications that share their location in a defined way for a particular purpose. And we already have a lot of applications that do that.

So I think we should be looking to that as the model for privacy protective use of location and looking for technical means, like changing Mac addresses, that actually don't require people to have their devices be observable and recognizable in every circumstance by everyone with a laptop.

JAMES RIESENBACH: I think it's early in a rapidly evolving industry from a technology standpoint, and it's important for us to keep in mind what's theoretically possible from what's practical and actionable and market driven in today's world. And so I don't dispute some of the hypothetical possibilities down the road, but we're in the business of helping real brick and mortar retailers compete more effectively and serve their customers better today. And that's where we keep our focus.

And absolutely we have to continue to evolve our technology, evolve our conduct. But at the end of the day, I think market forces prevail. And because those retailers or other businesses that violate the trust of their consumers will be punished by the marketplace more than anything else. And so I don't think that the reality is that some of the worst case scenarios will come to be because I don't think the market will allow it.

ILANA WESTERMAN: Yeah. I think-- I always look at it from the customer's perspective, from the user's perspective. And so they trust retailers right now. And then if you look at it from the retailer's perspective, are they going to try to compromise that trust? Why would they want to do that? I mean, do they want their customers to come back? Sure. Do they want to provide better goods and services for them? Yeah.

Everyone's trying to help each other in this particular environment. And that doesn't mean, I think to Seth's point, that there might not be other areas where harm can be done, but at the end of the day, the collection of information and the actual algorithms, are those bad things? I don't think so. It's the outcome.

And so I think we just have to always try to understand what do consumers really care about? Provide that transparency so they know if it benefits them or not so they can make a choice. And realize that we're at the beginning. I think James, to your point, that this is a hard problem. Trying to get people's attention, trying to provide that transparency, it's not going to happen overnight. We're going to do it but it's a process, it's a design process.

KRISTEN ANDERSON: Thank you. Thank you all very much. Thank you to all of our panelists for joining us today. It's been a great discussion. Thank you to all of you for participating and thanks to those who've been viewing the webcast.

We hope you've enjoyed the discussion today and we'd like to take this opportunity to remind everyone that we are accepting public comments on this topic until March 19. You can find instructions for submission on the web page for this seminar. Also, for our in-person audience, our chief technologist Latanya Sweeney will be conducting her demonstration again in the hallway just outside of this conference center. So if you didn't get a chance to see it on the way in, you can go and see that now.

And finally, we'd like remind you that this was the first in a series of three spring privacy series. The second will be on alternative scoring and that will take place here on March 19. The third will be on consumer generated and controlled health data, and that will take place on May 7. Thank you all.

[APPLAUSE]