FEDERAL TRADE COMMISSION

SPRING PRIVACY SERIES

CONSUMER GENERATED AND CONTROLLED

HEALTH DATA

MAY 7, 2014

W E L C O M E

MS. HAN: Hi, everyone. Good morning and thank you all for joining us for the Spring Privacy seminar, the last in the series of three the FTC has held to explore how emerging practices and technologies are impacting consumer privacy.

I'm Cora Han and I'm an attorney in the Division of Privacy and Identity Protection and today we're going to be talking about consumer-generated and controlled health data.

But before we get to that, there are a few housekeeping measures that I've got to get through. First, anyone who goes outside the building without an FTC badge will be required to go through the magnetometer and x-ray machine prior to reentering 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 need to orient yourself to New Jersey Avenue. Across from the FTC is the Georgetown Law Center. You'll look to the right front sidewalk, that's going to 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.

In the event that it is safer to remain inside, you'll be told where to go inside the building. If you spot 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 one of the Commission's publically-available social media sites.

If you would like to submit a question, question cards are available in the hallway immediately outside of the conference room. If you have a question, fill out your card, raise your hand, and one of our paralegals will come and get it.

For those of you participating by webcast, you can email your question to consumerhealthdata@FTC.gov, tweet it to #FTCPRIV, or post it to the FTC’s Facebook page in the workshop status thread. Please understand that we may not be able to get to all of the questions.

So now we'd like to welcome Commissioner Julie Brill to the podium for some brief welcoming remarks.

COMMISSIONER BRILL: Thanks, Cora. I want to

be really brief because this is a great topic. First of all, it's great to see so many of you here and thank you for all of you who are watching on the web.

This is an incredibly important issue. Those of you who know some of the things that I talk about when I go out and speak and write know that this is an issue, the issue of consumer-generated health information, is one that is near and dear to my heart.

So let me just really briefly paint the big picture and talk about the benefits and some of the concerns, which I know you are all thinking deeply about and I hope you'll keep in mind as the day progresses.

Big picture, consumer-generated health information is proliferating. Not just on the web, but also, of course, with respect to connected devices, the internet of things, or as Cisco says so famously on all the TV shows that I watch, the internet of everything. The potential benefits to consumers are significant. The potential benefits to society are incredibly

2.to shing.

specifically on health information.

Some of you know, because you were there as well, I was at the consumer electronics show in January and was really wowed by much that I saw. Some of the devices that I saw were particularly focused on health and the measure of life, quantitative life.

One in particular that really struck me was the Mimo. It was a onesie that was developed to measure the heartbeat, respiration rates, and other vital signs of an infant, a newborn. And it could send information to an app, it could send information to the parents' mobile device and whatnot. And think about the benefits of anyone who is worried about SIDS, any parent that might be worried about SIDS, or just might want to get their baby to sleep better or get themselves to sleep better, monitoring some of these important vital signs would be a real benefit in all of those areas.

We've seen tons of wearable step-counters, mileage monitors. There have also been some interesting articles about doctors who are finding out more about their patients by going online, Googling them. There was a New York Times Well-Blog post on that.

Or an interesting ethical debate underway in

the medical community about whether doctors should become friends with their patients on Facebook or other social media.

And then of course, another topic which I'm sure will be discussed today is the now infamous example of companies that are generating their own health data about their customers based on purchases, such as Target did with respect to its pregnancy predictor score.

So you know, again, taking a step back and thinking of the significant benefits that consumers can gain from some of these devices and their ability to measure their health conditions and what not. They can monitor their health, they can monitor their family members' health, in the event that they have an elderly parent or, again, the young child.

They can find the motivation to exercise or eat healthier foods. They can connect with people who have a similar medical condition or disease. They can participate in research. All incredibly beneficial.

But again, when health data is stored outside of silos, outside of the HIPAA silo that was created a fairly long time ago now, it seems like eons ago, in terms of the digital age, it will be health data that is not being controlled by doctors or hospitals or

insurers.

It is -- I think, you know, when you look at HIPAA and you look at HITECH, for instance, there seems to be a consensus in this country that health data is sensitive and does need special protections. And then the question becomes though, if we have a law that creates these protections, but only when they're flowing in certain contexts, but the same type of information, or something very close to it, is flowing outside of those silos that were created a long time ago, what does that mean? And are we comfortable with that? And should we be thinking about breaking down the legal silos in order to better protect that same health information when it is generated elsewhere.

Of course, there is also the problem of reidentifying individuals through information that had been de-identified. Latanya Sweeney is not going to necessarily talk about that today, but we so love having her here at the FTC. She is one of the nation's experts, as many of you know, on that very issue and so many other issues.

There are some other interesting things that I've read about, and I don't know if people will be talking about this today, but we've recently read that one insurance company, Aetna, has developed an app

Now some consumers would think that's great. Hey, you know, yes, I'd like to be part of a clinical trial. But other consumers were really shocked when they got contacted by this company, or others that got the information from the company, saying, you know, what makes you think I'm obese? Or how did you know I was a diabetic? Really interesting issues.

So again, I'm really looking forward to the day. I'm going to sit here as long as I can and I'll say hello to as many of you as I can during the breaks, but my plan is to sit here. And I know there will be a deep discussion about all of the new health data that is being generated by new devices and online services and apps. And I know we'll be exploring the benefits, because the benefits are significant, and do hope we'll also explore the risks.

And I would like everyone to keep in mind that health data, from my perspective, as one Commissioner, is highly sensitive, even though it may not be created and operating within a HIPAA context.

So with that, I'm really looking forward to the conversation. And thanks so much to Maneesha, to Cora, to Kristen, and to others for organizing this great day. And welcome to all of you.

Thanks.

MS. HAN: Thanks Commissioner Brill. To begin the program today, we're going to start off with a presentation by FTC Chief Technologist Latanya Sweeney

work I do is, if you have that kind of control over your information, how do you make decisions and how do you know that those decisions won't cause you harm? After all, how did their decision-making compare to a lot of the regulatory-type decision making is one of the questions.

And so my slides must have just stopped, so welcome to the world of Power Point. I'll just skip ahead.

So I think when we think about health data, it's really -- for most people, it comes down to the relationship between the physician and the patient. If there's not trust in that relationship, then the patient risk of -- the physician does not get all the information, the patient may hold back information. And if the patient holds back information, they risk not getting good care.

So I think we all understand the need for a kind of transparency and honesty of information going there, but what we don't always know is where the data goes after it leaves there, independent of other places the individual might post the data.

So a couple of years ago, we started a project at Harvard called thedatamap.org. And our goal was to try to document all of the flows of data. After

all, health data has been going around for a long time, where are all the places it goes? And to our shock, it is really not clear. It's not easy to know all of the places it might move.

So we've used all kinds of devices, mining web pages and notices, mining breach notices, breach notice databases, and also issuing public requests. So if there was a government agency that was somehow getting the data, we would then issue a public request to ask to whom did they give it, what's the data and so forth.

Now, we weren't the first group to try this. In 1997, there as a commission headed by Paul Clayton at the National Research Council who attempted to do this and this was right in the middle of the HIPAA debates. And they sat down and, through the committee, began documenting all the places the health data may go.

And it's kind of interesting. This is a model of their graph and you see all of the places that you might think and then some of them might be a little surprising.

So with our efforts, this is what it looks like today. Sort of eight years after HIPAA. And when you see, not only is there an explosion in the number

and types of data being given away, but also there is also just different kinds of entities receiving the data. If you visit thedatamap.org, you can actually click on any note and it will give you actual instances of how we came to know -- it will give you the company and what it is that they're doing.

Another question -- once we had this map, we began asking questions. So one of the questions is, which of the flows are covered by HIPAA and which are not. And to our surprise, about half of the flows are not even covered by HIPAA. So it's kind of an interesting -- sort of right away we saw an interesting issue that, when you asked -- when we surveyed students, the students said of the -- they expected that most data, outside of the data they give themselves, to be covered by HIPAA and we found that most were not.

One of the critical pieces there that you see is sort of in the middle there, called discharge data. So we began to focus on that, so a lot of pieces going out. And for most people, what the heck is discharge data anyway? Whoever or whatever this discharge data is, it starts from the patient, goes to the physician or hospital, and then it comes to this discharge data. How many people have heard of discharge data in this

room? Okay, so that's about half.

So whether you've heard of it or not, if you've been to a hospital -- if you have a hospital visit, and in most states physician visits, information about your visit is in discharge data. A copy of the -- these are mandated by state laws and a copy of that data goes to whoever is designated by that state law to receive that data.

And what you're seeing here on the data map is not just that they got the data, but you also see that they are either selling or giving away their data to others. The dash line means that they did so in a way that didn't have the explicit name, but it was, in fact, de-identified. That is, it didn't have name, address or Social Security numbers, but it included diagnosis codes, procedure codes, and how you pay for it.

So in fact, 33 states sell or share personal health data and this is a list of the states that do so. So then we can say to ourselves, okay, they are getting the data, they are selling it, they are sharing it, but how many of them adhere to HIPAA? And it turns out only three of them do. The other states are sharing and giving the data away in a way that's less protective than HIPAA, less protective than the way

HIPAA would describe how you might share or sell personal health information.

So one of the questions then is, well, maybe HIPAA is just too strong. You know, like maybe the federal standard is just kind of too high and there is nothing wrong with the lower standard that many of the states are using. Or is the case that the states should actually change their practices, and perhaps raise the standard to the HIPAA standards, for the stuff they commonly give away or share or sell. And then maybe have some other alternative if people needed more sensitive data.

So to test it, we went back to the data map and began to ask the question also, what might be harms if any of these questions posed out to be true. So one of the kind of interesting loops that we found was this loop to financial companies. So the data goes from you to the physician and from the physician to the district's data and then to a bank. That sounds really interesting.

So we looked at the literature and, many years ago, there was this article in the New England Journal of Medicine that described a banker who cross de-identified health data from -- about cancer patients in an attempt to figure out if any of them had

mortgages or loans at their bank and then began tweaking people's credit worthiness.

Now, I have no idea if that's true, but if we could show that it's possible by asking the question that that dashed line, how de-identified is that data -- is it sufficiently de-identified?

Another question that comes up is the online websites. You give information to a physician in a hospital, you give information to an online website, to what extent are the websites who are receiving the discharge data reidentifying you to the medical data that was left behind? And so this becomes a real interesting question because, at the time you're giving the data to the online website, you would have no idea what other data they might be pairing with it or what they might know. And if you click on them on my website, you can link to some of the companies.

So as I said, we gave out these FOIA requests for the top buyers and we listed the top buyers across states. And it's kind of a surprising list. You see a lot of analytic companies that most people have not heard of, you see WebMD, who has a large online website, you see IMS Health, who uses a lot of pharmacy data. We also see unions, which is kind of -- I don't know the story on that, but clearly there's a good

story there.

Okay, so let's figure out how de-identified is this data? Is it safe, is it okay the way they are giving it out? So for 50 dollars, we went to the State of Washington and we purchased their hospital discharge data for the year 2011.

And what you see here is just a sample of the 300 and some-odd fields of information for each visit. It included the age, in months and years, gender, zip code, and then you can see sort of what happened to the person, what hospital they went to, how they paid for it, and so forth.

At the same time, we wanted to find out a way to figure out how we might re-identify individuals to look at the kind of thing a banker might know about a person who had one or two things -- in other words, to what extent would that New England Journal of Medicine -- could it really be true? Could a banker do it?

Well, a banker and an employer and others know the same kind of information that often shows up in news clips about accidents. So we went -- so we took one news source in Washington State and just surveyed that one news source for news articles that were -- that contained the word hospitalization, or referred to hospitalized, and we got 81 samples.

And the typical story is like the one you see here. It often includes the age of the person, the city in which the person was coming from, where the accident happened. A lot of times they'll include the hospital and a description of the accident. But it doesn't include the zip code, which is with the health data.

So what you see on the left is, we just went to public records, given a person's age, their residence and their name, what are zip codes associated with that person? And these are just common public record sites. And then we do the thing on the second -- we take the stuff that we had from the news story, with the zip code, and we look for an exact match. That means, I'm going to take the fields, I'm going to try to match exactly those fields, and if I get one and only one match, we feel pretty confident that's the person, because state-wide collections is everybody, right?

And if we didn't get a match, we would relax one field and see if we then got one and only one match, because there could be errors in the news story. And we were able to correctly match -- exactly matching, this is not statistical, 35 of 81 of the news samples or 43 percent. And that's exactly the same

kind of information an employer would know about an employee taking time off, a creditor would know, family, friends or neighbors might know.

So let me stop there. Hopefully I've inspired you to think about some of the issues and questions that come up when individuals are sharing their data. Not to -- you know, the goal here is not to say that individuals shouldn't, but the goal is to figure out what are the risks and then jointly move forward about what do we do to move forward with the benefits, while addressing the risks.

Thank you.

MS. HAN: Thanks, Latanya. Next up, we'd like to take a closer look at some data sharing by some select health and fitness apps with a presentation by Jared Ho, who is an attorney in the FTC's Mobile Technology Unit.

PRESENTATION TWO: A SNAPSHOT OF DATA SHARING

MR. HO: Okay. Before we get started, a special thanks to Tina Del Becarro and the Mobile Lab for their support and expertise, to Cora Han and Kristen Anderson for putting this show on, to DPIP and the Mobile Technology Unit for their keen insight and input into this project. It was truly a collaborative effort.

So to get started, we started with the understanding that consumers reveal significant amounts of information about themselves when they use health and fitness apps. So this includes everything from basic information about the devices and the smartphones they are using, to the precise metrics and characteristics of their bodies.

So when we're talking about health and fitness apps and the wearables synched to those apps, those characteristics and metrics might include everything from running routes to eating habits to sleeping patterns to symptom searches, and even the stride or cadence of a person's walk or run.

Under this backdrop, we will take a look at a couple of studies that have already been conducted in this field. In July of 2013, Privacy Rights Clearinghouse examined 43 free and paid apps. They examined

the privacy policies of those apps, as well as tested the data transmission of those apps. They ultimately found that a large percentage of the apps did not have privacy policies, that about a third of the apps transmitted information data to a party not disclosed by the developer or the developer's website, and only about 13 percent of the apps encrypted all data transmissions between the app and the developer's website.

They ultimately concluded that health and fitness apps were not particularly good at protecting consumers' privacy. Since we did not review the privacy policies of any of the apps in our snapshot, we did not express any opinions as to Privacy Rights Clearinghouse's findings or conclusions.

Moving on, in September of 2013, Evidon conducted a similar study. They tested 20 health and fitness apps and found the presence of 70 third parties. They found that these third parties were typically advertising and analytics companies.

So this is actually -- this graphic is actually a picture of three third parties that received information from 14 different apps from the Evidon study. The blue dots represent the third parties and the cell phones represent the apps. So who are these

third parties and what kind of information are these third parties receiving about our bodies? And does the picture actually look different if we include wearables?

So we designed a snapshot to try to find out and take a deeper dive. So we looked at 12 health and fitness apps on one operating system. Two of those apps were apps that allowed us to sync information with our wearable devices. We tried to take a broad range of apps that gathered a variety of metrics about our bodies. This project was meant to be a small snapshot in time, so we looked at two daily activity apps connected to wearables, two exercise apps, two dietary and meal apps, three symptom checker apps, one pregnancy app, one diabetes app, and one smoking cessation app.

So using our Mobile Lab, we examined the information being transmitted from each app. While interacting with each app we were as permissive as possible, meaning that if an app asked us for permission to access a certain feature or to sync with another app, we always accepted and opted in.

We then mapped out the data sets to visually see the types of information being transmitted from each app and to whom this information was going.

different third parties. These third parties received a variety of information that generally fell into five categories. Device information, such as screen size, device model or language setting, device-specific identifiers such as a UDID, third-party specific identifiers, which you might think of as a cookie string specific to a particular app, consumer-specific identifiers, and consumer information, in this case dietary and workout habits.

So looking at it from another direction, we might ask ourselves what information are these third parties receiving from a variety of apps. So this is an example of a third-party ad servicing company that received information from four separate apps. We found that the same unique identifiers were transmitted to this third party from the various apps. We found that the apps also transmitted information, additional information, to this third party, such as at least one app transmitted key words such as ovulation, fertilization, pregnancy, and baby. So that essentially identified the type of app that it was to this third party.

At least one app transmitted gender information, at least one app transmitted workout information, and all of the apps transmitted basic

information about our device.

So while the third parties received the same identifiers that uniquely identified our device between apps, we don't actually make any determinations as to what this third party did with the information that it received from the various apps.

So moving on to our first observation, we found that 18 of the 76 third parties collected persistent device identifiers such as a unique device ID, a MAC address, or an IMEI. In some instances, the same third party received the same persistent identifier from multiple apps.

Our second observation, we found that 14 of the 76 third parties also collected consumer-specific identifiers. In most instances, this was a user name. A few instances, we found a name and email address being transmitted. It wasn't uncommon for a third party or an app to identify a user by their first name, a last initial, and then a string of identifiers.

And our third observation was that 22 third parties received additional information about our consumers such as exercise information, meal and diet information, medical symptom search information, zip code, gender, geo-location.

And finally, a summary of our observations.

Health and fitness apps collect and transmit to third parties sensitive information about our bodies and our habits. The 12 apps that we tested transmitted information to 76 third parties. The information included device information, consumer-specific identifiers, unique device IDs, unique third-party IDs, and consumer information such as exercise routine, dietary habits and symptom searches.

So there are significant privacy implications where health routines, dietary habits, and symptom searches are capable of being aggregated using identifiers unique to a particular person or their device.

PANEL DISCUSSION

MS. HAN: Great. Thanks, Jared. And now we'd like to welcome our panel up to the stage and we'll have the panel part of this.

MS. ANDERSON: Good morning, everyone. My name is Kristen Anderson and I'm also an attorney with the Division of Privacy and Identity Protection. Cora Han and I will be co-moderating this panel.

So our discussion this morning will focus on

Button enabled mobile apps, including iBlueButton and ICE BlueButton, working closely with the software development team.

Next, we have Sally Okun, who is Vice President for Advocacy, Policy, and Patient Safety at PatientsLikeMe, where she is responsible for patient voice and advocacy initiatives, participates in health policy discussions at the national and global level, oversees the company's patient safety initiatives, and acts as the company's liaison with government and regulatory agencies.

Next, we have Joseph Lorenzo Hall, who is the Chief Technologist at the Center for Democracy and Technology. His work focuses on the nexus between technology, law and policy, ensuring that technology

And unfortunately, our final panelist who was supposed to be here today is Heather Patterson, but she has been unable to join us. So we'll miss her input, but Joe Hall is actually familiar with some of her research and will do his best to speak about some of her findings and our other panelists will fill-in as well.

MS. HAN: So thanks to all of our panelists. We would like to start by setting the stage with why we are having this discussion about consumer-generated and controlled health data.

As Latanya Sweeney noted in her opening presentation, HIPAA doesn't cover all health data, but consumers may not know that. So Joy, I'd like to start with a question to you. Could you sketch out the boundaries of HIPAA for us and describe under what circumstances a consumer might generate health data that wouldn't be covered by HIPAA.

MS. PRITTS: I'd be happy to, thank you. Many people, not probably most of the people in this room, but lay people think that HIPAA covers all health information. They are familiar with getting the notice in the doctor's office and so they -- and also we see notices from people who aren't covered by HIPAA saying, we follow HIPAA.

But HIPAA actually is pretty sector-specific. And by that I mean, in this country, when we regulate information it really applies to the people, for the most part, who hold the information or who generate the information. In this case, HIPAA originally applied to health plans, most healthcare providers, and these things called healthcare clearinghouses, which were kind of essential to the transmission of claims data.

One of the interesting things about HIPAA that most people don't realize is that it really generated from a movement to standardize claims data. It wasn't really about privacy at all originally. Privacy was included as a protection, but the focus was on simplifying the administration of health claims and how they were processed.

When you know that, a lot of what happens under HIPAA makes a whole lot more sense. So the way it works is that HIPAA directly applies and directly regulates most of these healthcare providers and health plans. It puts limits on how they can use and disclose the information. So it really focuses on who holds the information and what they can do with it and who they can share it with.

The general rule is that they can't share it, except under certain circumstances, without the

patient's permission, except under certain circumstances. And there are a lot of exceptions under HIPAA which were aimed at trying to make the core purpose of providing health care and payment for health care easy and simple.

So you have health plans and health care providers. And under the relatively recent enactment of the Economic Recovery Act, there was a piece in there where Congress also improved the privacy protections. And that was referred to earlier by Commissioner Brill as HITECH. And under that Act, Congress expanded the privacy protections.

So you now have a situation where it's not just the health plans and the health care providers, but the protection also of HIPAA flows to people and organizations that undertake really core activities on behalf of those what they call covered entities and business associates.

So under HITECH, the data map that Latanya showed us a little bit earlier, it still presents a very interesting -- an interesting diagram. But there would be more solid lines, a few more solid lines, but it would also depend what function that organization is performing.

So for example, in that map, Latanya had an

HITECH contained a provision which really clarified that individuals have a right to get an electronic copy of their information when it's available. We think that this is a really important aspect of health care as we go forward. Because under the Affordable Care Act, patients are really putting -- are really being put at the center of their care. We are trying to move from a paradigm where health care is just provided on an episodic basis and really treat the patient more holistically.

But what that means is, in order to do that, you need information going back and forth between a doctor and a patient that is related not only to their doctor visit, but also to how they're living and what they're doing in the outside world, because then you get the entire picture.

One of the efforts to do that is to move that information to the patients. So patients do have the right to get access to their own health information. And the federal government has undertaken a number of initiatives to encourage them to do that. One of those is under the incentive payments for doctors and hospitals, under the Affordable Care Act, to adopt electronic health records. Some of the -- one of the key functions that they need to undertake is to allow

patients to view, download, and transmit their own health information.

What happens then is we have a -- we are encouraging people actively to move their information potentially out of the HIPAA-covered bubble and into the hands of others who may not be subjected to HIPAA. Having said that, there are circumstances, for example, when you have a personal health record that is offered on behalf of a health plan or a health care provider, because they are so tied to that plan and the provider, that information would remain protected under HIPAA.

If you transmit your information -- you know, you're a patient and you're looking at the website and you just find your own personal health record website and you say, hey, I want my information sent there, then it wouldn't be protected. So you can see how it's very -- it's a little complicated.

MS. HAN: Thanks, Joy.

MS. ANDERSON: Thank you. So turning now to some of the other products and services, like websites, apps and devices, that are increasingly putting medical tools and health data in consumer's hands, what are some of those products and what are their benefits? And Sally, if we may start with you?

MS. OKUN: Sure. Well, thank you very much.

You know, there's just such an array of them and we heard a little bit about that in Jared's talk, in terms of the kinds of apps and other devices, sensor devices, that are available to people today. So I think I won't spend a lot of time there because I think he gave us a really nice overview of that.

But I think what we need to be starting to think about is, first of all, the habits that people, as consumers, already have in using the internet, looking for information about their health. We know that nearly 75 percent of adults in the United States are already online looking for information. And many of those, about 60 percent of those, are actually looking for health information. So there's a variety of things that they're going to find there that could have varying degrees of usefulness and utility, as well as privacy protections.

So one of the things that I think is important is for us all to think about how we practice on the internet and where are we going. And that will help us to understand, I think, sometimes the kinds of things that are available.

So there's a variety of things. We have access to websites that are particularly focused on a particular disease, so you'll have a lot of websites,

really. There's a lot of things you can do there, in terms of transactional things like make a doctor's appointment or maybe check your labs, pull in some information, whether you are going to view data or transmit that information, but there's not a lot else to do. So I think consumers, in general, are looking for something a bit more interactive, a bit more informative, a bit more ubiquitous, in terms of being able to bring in other information about themselves in a meaningful way and then make some sense of that, with others often times like themselves.

So there's a whole host of ways of being able to find uses on the internet to start answering questions that you might have, either about your health, the health of others in your family or loved ones that you care about, but the variety of them are so diverse that you really have to start thinking about what's the purpose that I want to use it for and then understand what your risk might be in using it for that particular purpose.

MS. ANDERSON: Thank you. And Joe, did you have anything to add?

MR. HALL: Sure.

MS. ANDERSON: I know you've done some research.

MR. HALL: So that's a wonderful overview. There are a few things that -- it's a zoo of health and medical apps, devices, and websites out there. There are a couple that haven't been mentioned yet, so for example your phone can often integrate with things that provide some aspect of medical measurement.

So simple things like wireless scales that can upload your weight to a PHR or some other service. We have wireless -- there's one in the front row, I'm not going to point to the person wearing it, but there are a lot -- oh, sorry. She outed herself. But there's a lot of sort of recording your daily habits so that you can keep track of your health and wellness. And in some cases, these may be -- maybe not prescribed by a physician, but at least at the moment, recommended heavily by a physician.

And you have a sort of the vanguard of integration of sort of health, wellness, and medical tools. So there are, for medicine reminders, you have things like a pill you take every day that actually has a little microchip in it that interfaces with your smartphone to make sure that, if you have mental problems that may cause you to forget to take your medication, it will actually assist you in doing that.

And finally, there are really innovative

things that we really don't know what to do about yet. For example, Google announced Project Iris, which is a smart contact lens that will measure -- hopes to measure, I guess they would say, your blood glucose level by measuring that quantity in your tears. And if you put your Android device close to your head, it would let you know, oh geez, you probably need to take some insulin or something like that. So there's a real zoo. I'll be brief, because we have plenty to get to.

MS. ANDERSON: Thanks, Joe. And Chris, we know your company has a great product that we would like to give you the opportunity to talk about. So if we can see the personal health record in action, that would be great. So if you could give your demonstration?

DR. BURROW: Let me start by saying thank you to Kristen and Cora. And I'm delighted to find that the Commissioner is here. It's wonderful to meet you, Commissioner.

So I couldn't ask for a better set-up. HIPAA has been explained, but I chose that as my first slide. And I want to highlight what Joy said, which is that with HIPAA, we as citizens all have a right to our health care data. And with the updated version of HIPAA that you heard about in the HITECH Act, we all

have a right to electronic data.

And I like this memorandum that Leon Rodriguez has prepared, who is the Director at the Office of Civil Rights, so that any citizen who goes to his health care provider or hospital can take this memo and it really details exactly what my rights are as a citizen.

But one important thing about that memorandum is that it draws attention to the fact that, with new electronic health record systems and personal health record systems, patients can now help. They can now help to keep themselves safer and to keep medical care better. And so this is a very positive development and we are at the dawn of tools being offered to patients that can help them do just that.

So what I will hit very quickly is a description of the iBlueButton app, which Humetrix started building about four years ago. This is a native app that runs either on Android or IOS devices that allows you to take care of yourself and your family members by collecting health records either from places like Medicare or the VA or TRICARE or even now from hospitals and doctors' offices that have EMR systems.

And as you can see here, this particular

patient, I think I have the pointer, this particular patient has several records. This patient has a Medicare record, has a record that he has obtained from TRICARE, which is the -- TRICARE Online is the online site where active duty soldiers and their families can go get an online Blue Button record or their summary record. As well, this particular fictional patient has acquired data from an EMR system called Epic at the University of Caloa23rnia, Satai4wiegoaBdf/n/8

happened.

Now, this is a summary of the features of the system that we've created. And so on your left, you see the version of the app running just here on a -- I'm sorry, I'm going backwards, running on an Android device, but it's also on Apple device, where the user can download records from Medicare, VA, or TRICARE. What kind of records are those? They are called a Blue Button record.

You might see on my lapel, I have a Blue Button. This is the federal initiative that Joy was commenting about where the federal government, led by the Office of the National Coordinator for health care IT, has gotten together with a group and developed standards that allow individuals to safely, securely receive that data in a defined format for their benefit.

Now Medicare, along with the VA, led the way. And any one of you, if you're covered by Medicare or family members are covered by Medicare, can go to the MyMedicare.gov website, go through an authentication process there, acquire your log-in credentials, and then enter those into the app where they are stored on your phone. And you can download the record and the app will present it in a very user-friendly format

shown there, where you can see the record. And also, most importantly, what I didn't say in the last slide is you can push that record over to your doctor's iPad with a secure device-to-device data transfer, again, no data residing or persisting online, where the physician can see your data, plus any notations that you've made.

So we're giving you a secure way to receive your record, store your record, and share your record. And I just might say, in passing, that 37 million Americans who are covered by Medicare can use this technology today to receive critical information about all the medications that they've received in the last three years, that have been paid for through Part D, as well as all conditions that will have been coded for them by all physicians.

Now just to step back and let me tell you why I'm passionate about this. There are, in this country, somewhere between 100,000 and 400,000 deaths due to medical errors every year. There are at least 700,000 adverse drug events that result in injury or death. Just having your mom's medication record available to her when she sees her doctor, or you yourself having your own, goes a long way to preventing adverse drug reactions. This really can be critical, crucial information and we are passionate about delivering this

service to our users.

The new way to get data, you've heard about

you've received, as well as all of your conditions.

Just to finish up here, and quickly, because I think this is quite important, if you look at both medications and conditions, you can have a detailed view of your medication. You can tap this great resource from the National Library of Medicine, called Medline Plus, and instantly see side effect information about your medication. For your conditions, you can easily see information about your conditions, in English or in Spanish. And our app lets you indicate whether or not, for a drug, you are actually taking it or not, whether you are having any side effects or not, and would you like to keep this entry private. And the same thing for your conditions.

There are frequent errors in medical records. Our app lets you indicate if a particular condition is an error, whether it was in the past, or whether or not you would like to keep it private.

So the way our system works, when you share that data with your physician, if you're sharing the summary record, the only thing that they will see is the items, item-by-item, that you've decided you want to share.

Were you to share the entire Medicare record or the entire record from the VA, that record goes

across unaltered. So you, the consumer, are in control with this app.

So one thing I'd like to finish on is the privacy policy. So within the app, there is a privacy policy and you can see we also have an About statement and a FAQ statement that explains how to use the app. And if you tap on here in the privacy notice, you can see the ONC's model privacy notice that we put into the app, so you can see it right away. And this shows you whether or not we release any of your data.

Well, first of all, since we don't have your data, we cannot release it. So no, we don't release it. Do we require limiting agreements? Again, not applicable. And with regard to any particular details, we essentially don't release anything. So if we go back to the data map, I love the data map that Latanya Sweeney showed at the start, if we go back to the data map, this is a new kind of PHR. Pure PHR is essentially irrevocably tethered to you and only to you. You're not sending your data somewhere else, out in the galaxy of all those places, where there's a new data silo about you. Should you care to or choose to, you of course have a right to, but using this app, you don't have to.

So with that, I'd like to conclude. And

Kristen and Cora and everybody, thanks so much for giving us a chance to speak.

MS. HAN: Great. Thanks, Chris. So turning from the marketplace to privacy concerns, we spent some time this morning talking about data flows. And certainly, one of the most significant privacy concerns we've heard about is the potential for sensitive health information to be shared in ways consumers would not reasonably expect or anticipate.

So we'd like to spend a little bit of time on talking about these flows. I think we'd like to ask the panel, and perhaps Joe, you could start off and then others can jump in, could you tell us about the types of data sharing you've seen in the app world, as well as PHRs and elsewhere. And what sorts of business models are in that space?

MR. HALL: Okay, do you want me to specifically talk about business models first or talk about -- there are sort of two pieces to your question.

MS. HAN: Why don't you start with the sharing --

MR. HALL: Okay.

MS. HAN: -- and then we'll move on to the business model.

MR. HALL: So as Latanya's map sort of

showed, there is quite a bit of sharing in the traditional, sort of more clinical, medical service delivery, health care industry context. We don't know a whole lot about the sharing of apps, other than what was seen by the Privacy Rights Clearinghouse study, the Evidon study, and now the FTC is adding to that set of results.

But there's other research. So for example, Heather Patterson, who couldn't be here with us today, has done a really interesting, fascinating, qualitative study of Fitbit users. And if you don't like qualitative methods, well you're missing out and you may not like this work, but talk to me later and I would -- I have a degree in astrophysics, so I can tell you why they matter.

But anyway, the top concerns for people they studied using Fitbit, and you know it's pretty benign information. To some extent, how many steps you walked from an altimeter sense and then your actual motions

accidentally sharing individuals' sexual activity publicly or online without them knowing, because you don't typically wear your Fitbit when you're engaging in that type of activity, but you can self-report that kind of activity. And if you're sharing everything, you're sharing that as well.

That was very embarrassing to those users and Fitbit very quickly, to their credit, recognized that some categories of physical exertion may be a little bit more sensitive than others. I didn't even intend that to be a joke, so that's awesome.

But physical safety is another thing. So if you talk about routes, running routes and things like that, you may be able to predict where someone is alone or when they're not at home, and that can be extremely sensitive, given your own personal context.

And finally, employability and insurance ratings. We've talked a little bit about insurance rating, but to some extent these kinds of devices or these kinds of patient-generated or consumer-generated, I guess I should say, health data are increasingly being used in wellness programs to reward people or to encourage them to be more healthy, if not just for the bottom line, given your health insurance premiums. And other things as well, in terms of making it a better

working environment. And there's other things, but I won't talk about them.

But certainly in the business model side, and this is something that Chris may be able to enlighten us a little bit about, too, since he rolls with a lot of people who work in health apps, clearly the monetization models are not very different from health apps from other kinds of mobile apps at all.

So for example, there are things that are just purely ad-supported, and clearly the top 12 free ones that we see are those kinds of things. There are freemium apps and this is where you get something for free, but if you want some extra service, like knowing exactly what that drug does or something like that, you may have to pay a little bit more. There are sort of one-time payments, you know, you pay for an app and then you never have to pay again. And there are subscription apps, ones that feel that they provide such a service, and people pay for these things, that on a monthly basis you pay some money for that kind of stuff. And the ones that definitely seem to engage in a whole lot of sharing tend to be the ad-supported model ones, where you have an average of 15 different services, receiving various kinds of details about the user.

MS. HAN: Chris.

DR. BURROW: Sure. So with regard to the iBlueButton app, we have a “freemium model”. So for the consumer, the consumer, any one of you, can go on iTunes or the Google PlayStore and download the iBlueButton now and it's a free download.

Currently, since that version of the app that I just showed all of you is brand new, we just released it at this year's HIMSS conference, we are on special, it's absolutely free now. But coming soon, we will have the equivalent of a subscription model. Again, we believe that the client who pays for the app is, in fact, the client. If you're not paying for something, you know, you're probably not the client.

So we believe there is real value in letting people have access to this kind of tool, where there is absolutely no data sharing outside of the confines of your device. And so that's how we market this directly to consumers.

MS. PRITTS: Cora, I'd like to jump in and say that I think one of the areas that's kind of interesting is that people might say, “I'm willing to give you my information to get this product for free.” And they might not realize what some people, or some organizations, do with the information after they

receive it. So there's a certain amount of transparency, going back to the data mapping, what happens with the information after it is collected by the first third party. Because many of those third parties actually go ahead and resell the data to other entities. And sometimes that information is anonymized or pseudonymized so that it -- it would not necessarily have the individual's name attached to it. But some of the value in the information is being able to associate that information from that device with information that is collected from other services, such as your CVS card, your frequent flier card from Giant or Safeway or CVS or somebody like that. Or even your frequent flier miles. And there are data aggregators that are in the business of collecting this information, not from what we consider your health, your core health people who are in organizations that are covered by HIPAA, but by these other kinds of outside players in the market now, where people probably don't have a good idea that that's happening with their information.

MS. HAN: Thanks. So de-identification is definitely an excellent issue to bring up and we will be circling back to it a little bit later today, but I had another question I wanted to sort of follow up here

with and that's, to any of you here today, are you aware of self-regulatory efforts limiting the use of health data for online marketing purposes? What sorts of things have you been seeing?

MR. HALL: So I can sort of talk about that. I mean, there are a smattering of self-regulatory guidelines and codes and principles. The AMA, the American Medical Association and the American Medical Informatics Association have some guidelines for electronic communication with patients. That's very different than consumer -- it's very narrow compared to consumer-generated data.

The Decapg7bap2shealth euo pcee sse gui2hings have2srEnDni3Td (12)Tj

specific consent for somekinds of uses like behavioral, will require the user to give explicit consent before they can do things like behavioral advertising.

But there's nothing that sort of -- that I know of, and I'd love to be proven wrong, it's sort of more generic, you know, sort of guidelines for health apps that may or may not be using sensitive data. And I'd love to be corrected, but it's the kind of thing that I think the time has come.

MS. HAN: Thanks. Anyone else have anything to add?

MS. OKUN: I would just add that, you know, consumers themselves, when they are starting to use some of the features that might be available to them on our site, for example, I think Latanya had mentioned,

allyn e/Bre hayou 9now, i22 (spcogniced star8isthes trust. TdyAnd else of have anythin8)Tj -2.842 0 T

that are very prominently displayed to let people know, first of all, that their data will be used. We actually aggregate, de-identify, and then make that data available to interested parties. That might be pharmaceutical companies, it could be government, it could be clinical researchers, who want to learn from the experience of people living with chronic illness over time.

So we're very upfront about that and I think that that's something that's critically important. We also encourage people, in terms of our own guidelines, not to use their real names, to be careful about the kind of information they're sharing within the forum conversations, but also to recognize that it's their choice. And so we will often times see people with real pictures on the site. And it's not necessarily something we would promote, but we also recognize that that's the choice that the consumer themselves has made.

But I think the other piece is, in terms of our site, again I just want to bring that back, one of the things that we've learned is that, in terms of the data sharing research that we've done, is that, for the most part, people are really willing and interested in sharing their data for a couple of really important

reasons.

One is, they want to know, in our experience anyway, is my experience normal. They'd like to be able to share with other people like themselves to better understand whether or not what their experience is seems to be what other people like them might be experiencing.

One example is in epilepsy, we learned early on that about one-third of the people with epilepsy on our site had never talked to or met another person with epilepsy before, and it's a very stigmatizing condition.

The second most popular reason that they give is altruism, I want to have my experience benefit other people.

So I think we need to find a way of unpacking some of the ways that we can make it easier for patients to share this kind of information without necessarily compromising their privacy to the degree possible, recognizing that when you're on the internet, your privacy is subject to being revealed, and that's not something any of us can fully protect. But when consumers are aware of that in the most explicit and transparent way, I think we actually elevate their willingness and their appreciation of why sharing

health data can be actually quite beneficial, not only for them, but for others like them.

MR. HALL: I forgot to mention one thing that my employers would be mad about. So at CDT, we are also -- we're working on big data and health, and explicitly looking at the Fair Information Practices and to what extent they need to be tweaked, because we don't believe that they're irrelevant anymore. So that's an ongoing project that is going to take a good chunk of the rest of this year, but myself and Justin Brookman, the director of our Consumer Privacy Project, and Gautam Hans, our Plesser Fellow, are working on this and if you're interested in this, let us know.

MS. HAN: Thanks.

MS. ANDERSON: Thank you. Joy, there was one other aspect of unexpected data flows that we wanted to ask you about and that was in the context of electronic health records and the data that can flow from them.

MS. PRITTS: Well, everybody receives a HIPAA privacy notice. How many of you have ever read them? So people here have, but most of the time when you ask -- I will also tell you that we've done -- we have, in the course of work, not at ONC, but in my past life we did focus groups. There is information in those notices that people just don't read.

There has been a revised version out that puts patients' rights out first, instead of the uses and disclosures, to try to highlight some of those uses, but one of the uses of information that many people are surprised about is their use of health information for research. And there are ways that health information can flow for research purposes that happen without the individual's express permission. And that surprises a lot of people. It's totally legal, but it's surprising.

I think one of the ways that the research community is headed is very important for us, as we move forward, which is patient-centered outcomes research. And that's really looking to not only clinical trials, but looking at a person longitudinally to see, not only how they were treated, but how they are living, what activities they are undertaking, and after they've been cared, how did that care work and how were those health outcomes affected.

There are some organizations that have formed independent third-party organizations to really undertake this research and they have found that it's really valuable for them to collect the information, not only from the health care entities, but also from things like we mentioned a little bit earlier, your

Safeway card, your frequent flier card, your purchase data, your financial data. Because there are often correlations in the other types of data that, when matched with your health data, they believe may prove very informative about predicting what will work and what will not work with people in terms of treatment.

So it's something that I think a lot of people find a little bit surprising, how all of those little nodes on Latanya's map can also actually be brought together.

MS. HAN: Thanks. So building upon something that you touched upon, let's pivot a little bit and think about consumer perceptions of these data flows. And perhaps, Sally, I'll address this next question to you.

You were recently involved in an Institute of Medicine study regarding social networking sites and continuously learning health systems, which reached some interesting conclusions about social media users and the sharing of their health information and what type of sharing they are comfortable with and what type of sharing they may be less comfortable with.

MS. OKUN: Mm-hmm.

MS. HAN: Could you comment a little bit about that?

someone else.

But what we wanted to find out also was who were they willing to share that with outside of PatientsLikeMe and were they already doing that and also what were their concerns. And so we did learn a little bit more about what makes someone hesitant to share data outside of the walled environment of PatientsLikeMe.

Certainly, we've heard some already. Seventy-six percent of the patients interviewed thought that their data could be used without their knowledge. So we already know that it is being used without their knowledge, it's moving on to different places. So that actually validates that concern. Seventy-two percent were concerned about their benefits and being denied

those are things I think we need to be sensitive to.

But when we started asking, outside of PatientsLikeMe, who are you already sharing some of this information with? We were actually surprised at how little people were sharing. So given an environment where they felt safe to do this, they were ubiquitously sharing. But when we asked how many were sharing it with their spouse or significant other, only about 30 percent said that they actually share the information on their profile with them. And it went down fromcnhe

d58ddTaTj - -2.24bout 30 perc6nt said that7 d58clinicians

monitor moods and things like that.

And other patients -- outside of PatientsLikeMe, about 16 percent were willing to share with other patients. So again, when you start to get out of this environment where they felt a sense of trust, they were a little bit less sure that they wanted to.

And their children, only nine percent felt that they wanted to share this information with their children.

Now, not out of this study, but another survey that we had done a couple of years ago, we also asked what kind of information are you not sharing with your health care provider. And it was really quite not surprising, actually, to learn that they weren't sharing things about their sexual dysfunction or sexual health. They weren't sharing things about behavioral things, like drinking and that sort of thing, and not being quite as honest about their diet. However, when asked are you sharing the same information with your peers, on PatientsLikeMe, almost 100 percent said I am more comfortable sharing it here. It's anonymous, I feel like I can share that and be honest about it, and people can respond to me in a way that I can actually appreciate and then respond myself behaviorally.

So it was really interesting to start seeing how we share some things with some people because we are going to get some sort of reaction possibly, or not, and then with others because we might get some benefit back by sharing, that that might actually help us to be able to deal with whatever it was we were sharing that with.

MS. HAN: Chris.

DR. BURROW: Yes, I just wanted to make a comment. So one thing that we're finding is, and this is because some of our users call us up, we have actually no way of knowing anything about our users. I don't know any of their names, I don't know anything about them, they have all their own data.

But people do call us up and one thing that we're being told is that, with regard to physicians, we are now putting in the hands of patients a full medical data set. So let's take drugs: brand name, maker name, dosage type, dosage form, NDC code, every single date where it was ever filled, you have it on your app. You can share that with your physician. This is hard data.

And anecdotally what I'd like to say is, and I've had patients tell me this, it's so infuriating, when I go see my doctor now, he looks at his computer screen and he never looks at me. And he types and

everything. And suddenly, I have something on my screen and he'll have to turn around. Like, look at my screen.

Because now suddenly, we're at the dawn of this new age, and that's what we're passionate about, of giving consumers the actual wherewithal, technologically, to have a complete, or as complete a data set as possible today. And so that's suddenly putting consumers in a much more powerful position to help their physician take better care of them.

So this is, you know, the start of something new and very, very important. Technology, very sophisticated, in the hands of patients that they can use to be helping with the health care system, instead of just being passive recipients of health care.

MS. OKUN: Can I just follow-up on one topic there?

MS. HAN: Sure.

MS. OKUN: And I think it came up before. One of the things that patient-centered outcome research is doing is sort of suggesting that we actually start making use of routinely collected data at the point of care. And we're not necessarily doing that well, in terms of quality improvement in continuous learning.

So this is something that, as consumers, we can be teaching people that it's really important for you to understand that, as we collect routine data at the point of care, we are going to start trying to make use of that so we can start to understand things from a comparative effectiveness perspective and that sort of thing.

What we also now need to start doing is have policy and clinicians catch up with patient-generated data, consumer-generated data, to say, this has value at the point of care, it has a unique perspective we previously have not collected, and we have to find ways of being able to expect that that data will be respected and honored at the point of care, while at the same time not overloading clinicians so that it doesn't fit into their workflow.

So we, as app developers or website owners, and then people who are working from this perspective, have to understand that the clinicians need to receive this data, inform us that they can make use of it, and not feel that they're overwhelmed by it, so that we have a balancing going on there.

MS. ANDERSON: Thank you.

MS. HAN: Thanks. Joe, did you --

MR. HALL: So I'm going to put my Heather

with people they've never met because they don't want anyone knowing about their regular daily habits. So there's a really interesting social divide with how people are using these kinds of tools.

And the fascinating thing is people are thinking a lot about how Fitbit's, specifically, business model might change. And so they don't know what may happen in the future and, in some cases, you see worries about things like, you know, who has access to the data, who has potentially access to the data, does the government have access to this data? Under what circumstances can a -- you know, if there's a fist-fight in a bar, can the accelerometer data be subpoenaed off of my Fitbit to prove things about -- you know, whatever.

And so there's a whole bunch of interesting

notice and what are some of the ways of meeting those challenges? We hear a lot about information asymmetry resulting from poorly crafted or very long privacy policies.

Joe, would you like to start us off?

MR. HALL: Sure. It's often said that notice and choice is -- or notice and consent is dead. We at CDT don't believe that. And what people tend to say when they say those things are, no one reads privacy policies, and that's so true, except for a few of us who, for some reason, get a kick out of it, right? I guess there are people that it's part of our job, we have to read these things.

But at the same time, if you're expecting people to read 30 pages of legalese and understand it and be fully informed, you're going to have a bad time actually communicating with people about what you're doing, but that's why there are a bunch of other efforts. So for example, there are some platforms, like Apple's iOS platform that use just-in-time notification. So if this app is trying to access your location data, yea or nay. And if you say nay, then

things like directions and stuff like that.

There's also, as I mentioned earlier, an effort at the NTIA, the Mobile App Transparency Code of Conduct, that focuses on short notice. And there's a whole lot of academic research that is evolving and tends to be sort of on the short notice. Even short notice is very hard to communicate effectively with people, but I'd like to think that the NTIA process, which shows, here's the data that's collected about you using this app, here are the entities with which the app shares this data, on one screen or a couple of screens of easy, popping, sort of interactivity, I'd like to think that that will evolve and be something that people tend to recognize. Sort of like a nutrition label, you know, it's something you know where it is, unless it's something that's too small to have a nutrition label on it. You can find it, you sort of know how to interact with those kinds of things.

In the longer term, I do think it would be neat to have just-in-time notification for storing and access health data. So if we could get mobile platforms to actually carve out a little chunk of its operating system to store things like, you know, a CCD, a common care -- I forget what the acronym stands for,

a summary of your clinical interaction. And then the

not sure that people really read soup cans that much, Joe, but --

MR. HALL: I do because I'm hypertensive, so.

DR. BURROW: That's a great idea. And so there are no's and yes's that are pretty clear there. I think there needs to be those kinds of simple notices to make it clear.

I might want to set you up again to come back to de-identification, because I also read privacy policies. Ours is simple, it's one page, but I've read other privacy policies that say that we'll share data, but it will be de-identified. But they don't specify what that term means. And you know, I'm also a scientist and so, gee, I wonder what that means.

MS. ANDERSON: Right.

DR. BURROW: So I think there's a problem with transparency there.

MS. ANDERSON: And we will definitely get more in detail in de-identification in just a bit, but I think there's a -- there's a second component to the transparency, notice and choice thing and that is about contextual use of information.

So you might have a soup label type of notice

13up fm of noTaabel tyI thins,n-Te-es afor.will def

you have mentioned that as well, so what about when data about patients is linked or re-purposed after the fact? So it might be covered in the privacy policy, but then used after the fact. How do you work to provide effective notice and choice around that?

MS. OKUN: I can speak to PatientsLikeMe. I mean we, actually in our privacy policy, transparency and openness statements are pretty clear that the data that you are going to be providing will be and can be used for aggregation, de-identification, and then shared with our partners, whomever it is that we're working on a project with.

That said -- so that's the basic profile data. That said, when we are actually in the process of working on a particular project or we're doing an initiative or survey study, that reminder comes in as part of the consenting to participate in that survey.

So that information would clearly tell them who our partner is, it would clearly tell them how that data is going to be used in the context of this new survey or study that we're working on, and we also promise them to give that data, the findings from that data, back to them within a reasonable period of time. That's a promise we make with almost everything that we do. It's a sort of give something, get something mantra that

we have.

So every time you give us a piece of data, we either give you a graphic display of what that data means, in the context of everyone else on the site, or when we're doing a specific study that is targeting a particular set of questions we will bring that data back to the users, either in a blog post or forum or in some format for them to be able to know, here's what you contributed, here's what the findings were, and then generate some conversation about that.

MS. ANDERSON: So we've also heard about privacy being a shared responsibility. We've heard a little bit from Sally and others about that and we just wanted to follow-up a little bit about what consumers should be doing, if they only have control over, say entering the information once into the app that they're interfacing with right then, and then it goes on to be shared on the back-end. How can they keep their data in the context that they would expect?

MR. HALL: So it's a double-edged sword with no handle, so to speak. Well, maybe that's not right. It's a double-edged sword of, view, download and transmit. View, download and transmit is awesome. People have their data in their hands, they can do a bunch of stuff with it.

The double-edged sword part of this is that people can do really silly stuff with their own data now and they can do things that are sort of irresponsible. But that's part of sort of this national sort of negotiation process that we're having with increased custody, so to speak, on the patient's side of being able to use and do things with this data.

And so if any of you ever see someone post their medical record on Facebook, that's a really good opportunity to have a conversation with that person about what's appropriate and how, you know, that might not exactly be the thing that you want to read, being an audience member for that person's Facebook profile.

But I think there is a whole set of social practices, in terms of people that are thinking about things, that are more knowledgeable about these things, you should really keep your eyes out for that sort of stuff. But consumers in general are going to need to think harder about these things. There are going to be some fantastic mistakes that happen that will serve, for folks like us, who are consumer advocates, can go out and say, look, don't end up like this. Please protect your information more like that.

And on the NSA Snowden side, we're doing a whole lot of stuff making sure that people can properly

protect their data, be it in a communications session or data at rest, you know, stuff you have on your computer or your mobile devices. And so I think there are larger trends that everyone needs to sort of bone up on their digital hygiene, so to speak. Understand things like password managers. You know, I have 1200 passwords, I only know two of them. You should never have to know more than that because there's really good tools that will help you create secure ones and you'll never have to remember another one again. There's a whole slew of sort of things like that that, as a society, we're going to have to learn to incorporate into the fabric of how we do things.

MS. PRITTS: I think that one of the issues that I continuously hear is that there are many people who think, from a consumer perspective, that privacy is dead. Nobody cares anymore. Look, people share all this information on Facebook, they engage in this behavior on social networks, so they don't really care.

I think there also are a lot of research studies that have come out within the last year or so that really question that perspective. Because people who have had something happen to them, or know something that has happened to somebody due to information that was posted on their website, or

something of that nature, have a renewed respect for their own privacy and how their information may be used.

I also think that people -- there is a segment of people who care a lot about privacy and there are people who would share everything with anybody. Again, sometimes those perspectives change when you realize what the consequences of that sharing might be.

I also think, when you hear this conversation, it's like, well, only 10 percent of the people in America really care about privacy. But that 10 or 20 percent is flexible. It's not a static number. People come and they flow into and out of, you know, how much and whether they care about how they're sharing their information, depending on, again, the context.

So I think there are a lot of nuances to the discussion about, first of all, people's perspectives on privacy and what they're willing to do to protect it. Some people have a lot more at risk than others do and that changes over time. It's a very dynamic issue.

MS. ANDERSON: Did anybody else have anything to add to that point?

MS. OKUN: I would just add that I think that all of this is so true. And I think we're entering a

time when consumers are going to be expected to have a lot more ownership of their own health and their health care. And whether you want that responsibility or not, it's coming your way.

So I think there's a lot on all of our parts to be able to start thinking about what is it that I need to know, who do I need to learn it from, and where might I get this information to start protecting myself. I think it's just very clear that we probably can't protect ourselves from a lot of this third-party push that's going on. Because first of all, we may not even be aware of it. But when we do become aware of it, we begin to have an increased sensitivity, I think, as Joy has already said.

But I also want to reinforce that, even people with chronic illness, who are participating in data sharing significantly on PatientsLikeMe, have an expectation that we protect their data. They have an expectation that we anonymize that data and that we de-identify that data. That expectation is something that, again, as I said earlier, were we to violate, we would be not able to have the trust of our patients.

So I think that there is an expectation, especially among those who feel that they have a lot to lose, if some of that information were to become

that's up-to-date can avert all sorts of medical misadventures and catastrophes that you, your children, or your parents could be subjected to without this data. So there's a tremendous benefit, as well as a privacy risk.

MS. PRITTS: And we won't see that benefit unless you protect the data.

DR. BURROW: Yeah.

MS. HAN: Okay, thanks. So we'd like to move on to de-identification, which has come up a couple of times today.

And first there was a question from the audience. So there's talk, and this is what we've been discussing a few times, about sharing data in de-identified form. So could people comment on Latanya's finding that her group was able to reidentifye comment on 12

birth, month, day and year can identify 50 percent of all Americans. That's pretty extraordinary. So there is a real need to have ways of avoiding putting those three, just those three simple facts together.

MR. HALL: I was just going to make one slight correction, which is Latanya's original study showed a higher number than that. I think it was 70-something and then there was a follow-up using the 2000 census data by Philippe Golle, which dropped that down to like 60-something, so it's big.

MS. HAN: Thanks.

MS. PRITTS: I think there's a large variability in how de-identification is defined.

MS. HAN: Oh thanks, yeah. I was going to follow-up with you about this.

MS. PRITTS: So I think the HIPAA Privacy Rule probably has one of the most stringent definitions of de-identification of any privacy rule that I've ever read.

The paradigm in protecting health information, or any kind of information, is drawn in just every statute, regulation that I've ever read and it's limited to identifiable data. If it's not identifiable data, depending on how you define it, then the regulation or the statute generally doesn't apply,

because the idea is to protect the individual, not just random data.

So the question then is, when does information become identifiable to the point where you can actually attach it to somebody. And that is kind of a moving target and that has changed, and will continue to change over the years and as technology advances.

So the privacy -- the HIPAA Privacy Rule has two means under which information can be considered de-identified. One is a safe harbor method, where you have to remove many of the elements that Chris mentioned earlier, which are almost all dates, you know, zip codes, name -- the obvious ones, your name, your Social Security number, the medical record number, to the point where, during the comment period when the rule was being written, as some in the audience would attest, there was a big blow-back because researchers were saying, we couldn't possibly use this information because we can't associate it with anybody and we need to do longitudinal, longitudinal associations.

So in the Privacy Rule, it's kind of tiered. There's also a tier of information of which the major obvious identifiers have been removed, but many of the other information can still be retained, such as dates of service. And that information -- there's a

recognition that there is some potential there for re-identification, so that information can be shared, particularly for a researcher, to disclose for research, with a data use agreement that the recipient won't reidentify it.

And that is one of the ways that people are addressing this issue is, kind of stratifying the information. And you'll see this on public-use sites and I think NCI did this as well, the National Cancer Institute. Here's information where we believe we've done a really good job, and there's some testing done to see how good a job that they've done, and that information is available in a public use file. And then information where there is larger potential of reidentifying the information, they make subject -- they make available, but it is subject to some sort of a data use agreement.

Having said that, some of the information that was -- for example the state release of information, is from entities that aren't necessarily subject to the HIPAA Privacy Rule. For example, public health departments in states, it's a complicated issue, but many of those are not covered by the HIPAA Privacy Rule. They are often, though, covered by their own state laws. And how state laws define what kind of

information can be shared or how it has to be anonymized or de-identified vary very much. And they, too, are sector specific.

So what it says over here and the rule that governs doctors or other health care providers may be different than the equivalent of their privacy act. So de-identification, there's not a single rule that governs everybody.

MS. HAN: And that was actually going to be my follow-up question. This is something, Chris, you also referred to. There is no standard definition of de-identification sort of across the various products and services.

So here's the question for the panel, should there be? And if so, do you have thoughts about what it should be?

MS. OKUN: I'm going to say probably yes, there should be. I'm going to say that there should also be, within the business model of the company, some inherent responsibility for acknowledging the ability to reidentify information that could be used inappropriately.

And so I'll speak to that from PatientsLikeMe's perspective. We are not a regulated entity under HIPAA; however, we adhere to the

de-identification processes on restricted data and protected data, and that's part of our standard operating procedure. So any time we're working with a partner, they understand that. They understand that the data use agreement that they will sign with us, in terms of receiving information, will be free of anything that would be considered that.

Now that said, within our environment of working with them on a research project, we will take that into consideration so that that usefulness of that data could actually be considered in the context of whether we want some geo-coding kind of information to understand what are we looking at regionally and that sort of thing.

Also, within our own company, we hold each other to different levels of access. So not everyone in the company has access to all of the information. Those of us who are in the process of doing certain research activities, or data science activities, will have different levels of access. And that's also spelled out quite clearly in our standard operating procedures.

So I think there's a certain level of responsibility that companies do need to rise to, even when you're not a regulated entity, and start thinking

about what that responsibility looks like. I'm not one necessarily to say, we need more regulation. But possibly we need guidance and policies that can help frame this conversation more so that it's more transparent to consumers.

MS. HAN: Others?

MR. HALL: Sure. At CDT, we're a big fan of the FTC’s de-identification -- I don't know if you call it a standard, but sort of a rubric or a guideline. And I actually forget the first two pieces of it, but it does things like it binds downstream recipients. You have to enter into a contractual relationship to make sure that that downstream recipient doesn't do certain things like try to reidentify stuff.

I don't know. A standard could be really difficult. It's sort of generic in the sense that, you know, being a privacy and security guy and a guy who spent my Ph.D. hacking voting machines, for example, you start to realize that some of these things are case-by-case kinds of considerations. And in de-identification, you want to think about the utility that is going to, you know, that you want to retain in the data. And you can't really do that in a generic way.

And you also want to think about the threats,

And I'm also a big fan of the version of the HIPAA de-identification that isn't, remove these 19 identifying kinds of quantities, but you know, engage with an expert to actually probabilistically determine, given your use, to what extent these might be re-identifiable. That's a little hard, and expensive, because you have to engage with an expert and there's not a lot of people who do that. You go to try to find more than two or three of them and it gets pretty difficult pretty quick. And we try to do that when

transparency on this issue.

MS. HAN: Thanks. So we have another audience question. How do the panelists think we can come to a common definition of what information and when information is health information?

MS. OKUN: I'm not sure we can. First of all, from a consumer's perspective, we all value and quantify our health in different ways. So what I value as being part of my health picture may look differently than it does to someone else in the room. So I think there's probably certain psycho-social kinds of parameters that will apply to health broadly. And then there's physical characteristics and mental characteristics and all that apply to health broadly. But then when you start thinking about health care, I think you start talking about very specific and different things.

So talking about it from a consumer's perspective, and asking them what constitutes their health, might look very different than if you are talking to a payer or a clinician as to what constitutes health. So I think coming up with a common thing that is going to cross-cut would be probably pretty challenging. I think we need to recognize that health means a lot of different things to most of us.

And finding ways of being able to understand that and put that into context, I think, is probably more important.

DR. BURROW: Certainly, there are core things that we all agree are health care data. Your names of your medications, the names of your medical conditions, your allergies, the immunizations you've had, the treatments you've had, the surgeries you've

DR. BURROW: It's required, but not sufficient, right?

MR. HALL: And to elucidate that a little bit more, when I was a post-doc with Helen Nissenbaum, you may not have known that you are pulling your panel from a similar team, but Heather couldn't make it, so now it’s just me.

But we did a study of gay males and MSM, men who have sex with men, just to -- this is a population that guards their health information very carefully, because it's not something you can tell by just looking at them, and there have to be very specific kinds of circumstances in which they feel comfortable talking about their health information.

The sample we talked to was 30 men of a pretty stratified age group, very young and very old, and we found extremely surprising things. Like most of these men, we didn't ask the question but it was clear that they were HIV positive or had AIDS, and that wasn't so much of a big deal, sort of how AIDS has developed now and HIV has developed now, in the sense that, you know, it's a manageable disease. It's kind of like something that everyone has to know if you interact with folks, even in a nonsexual manner.

But there were things that they found really

sensitive that we could never predict. So for example, one of them was really concerned about his sister who was 25 and still wet the bed. And that was such a sensitive thing that their whole family was -- part of the way that they operated was making sure that they protected that kind of stuff and making sure there was always someone who was indoctrinated into how to manage that condition with her at all times. So if she was out at a bar drinking and passes out, red lights go off and you need to make sure that certain things happen.

But that's not the kind of thing we would have ever predicted, and those are the kinds of things they were really concerned -- because the whole study is about, as we go from paper records to electronic medical records, does that affect the ability -- their tendencies to disclose information to their physicians. And those are the kinds of anecdotes they told us about, things I had never thought of that we could never sort of encapsulate in the data structure, and that's sort of this human element that I think inevitably will evolve, as society and culture evolve and as, you know, our health delivery system and technologies and techniques we use to do that stuff.

MS. ANDERSON: Thanks.

MS. PRITTS: I think the recently released White House report on big data makes a very good point when it points out that, what is health data and what is financial data and other types of data, is really merging. And as we accrue this data and collate it and use it, it is going to be harder and harder to draw that line of what's health and what isn't.

I think that people's spending patterns, for example, would never occur to you to be your health data, yet that information may be used at some point to treat you and then it does become your health information, doesn't it?

MS. ANDERSON: Okay, unfortunately we are just about out of time so we just wanted to give you each a minute to close by sharing your thoughts about -- especially if you have any thoughts about best practices, to protect consumers privacy and security of their data in these contexts. You want to start first?

DR. BURROW: Well, I think it's been a great discussion and we've really focused on unexpected and, to consumers, unknown data flows that, by these modern devices that we are all now acquiring, can leak out and maybe come back and have important effects.

We've also heard that patients don't read privacy notices. Or consumers don't read privacy

notices. So I think we all have to work together to come up with some easier, better, more consolidated way to signal to people what are the risks that they're taking with their data and how they might mitigate those risks and then each consumer chooses.

On one end, the Humetrix iBlueButton solution is providing, if you will, your own lock case for your own data that stays with you at all times and you are completely in control of that data. On the other hand, the Facebook example, if you are unwisely posting a lot of identifiable data there, that’s really a bad choice. So I think it's going to be situational.

And with regard to devices, and specifically to apps, I do believe there needs to be better and clearer information in the privacy policies presented in a very simple, graphical format that will give you a heads-up display right away when you are using the app.

MS. OKUN: Thank you very much and this has been a delightful panel to be on. I'm actually looking around the room thinking I bet people have questions and it would have been fun to get into some of those, too. So so much to cover and so little time.

I think, from my perspective, the most important last comment I would like to make is that we have to really try ways of reinforcing the value of sharing

information to continuously learn about how to improve health and health care in this country. And trying to find ways to do that by engaging with people and consumers on a regular basis about that value and making that value equation come to life.

So shared data, along with shared -- sort of allows you to have a more robust shared decision making process and ultimately allows us to have shared accountability for the outcomes that we have and also the disposition of the data. So I think it's a really important piece that, as consumers, each of us needs to start thinking more concretely about what is it that is constituting my role now in my health and health care, my family's role, my children's role, my grandchildren's role. How do I help them appreciate and understand that value, while balancing and finding that area, that sweet spot, that says I'm exploring the risks as well and I'm beginning to understand them better.

But I do think we need to start holding a higher level of accountability around the use of apps and things that are sending data in places that may not necessarily be in our best interest. And until we can do that, I think, as consumers, we need to be much more aware of opting in, as Chris said, or opting out when

it seems like our safety or the access to our information might be at risk.

MS. HAN: Thank you, Sally. Joe.

MR. HALL: Yes. Thank you Cora and Kristen and the FTC for holding this forum.

Similarly, I definitely think -- the thing that -- and this is almost a full employment act for myself. What happens all the time is that when people want to do something cool, make a health app, make a thing that does something fun, they inevitably don't think about a lot of these things, unless they're developing a privacy app or something, right? A privacy and security app.

And so it would be really nice to have frameworks and have people develop sort of not just guidelines and stuff, but development environments and technical tools that will allow people who have a cool idea to not have to worry about some of the -- I mean, to some extent, you want them to worry a little bit about that, but it would be great to sort of obfuscate away some of these core security things. And security and privacy aren't that different in that security enables you to protect your privacy.

And so I'd really like to see something like that that would -- and I don't know who I'm asking to

do that. Maybe it's us, for example, in cooperation with some of the app industry folks. Because we want people to make cool stuff, but we also don't want to keep on having these common failures. And I don't want to rely on enforcement entirely or the press entirely to sort of shame people into doing the right thing, but actually have some things that are embedded into how these tools are created.

MS. HAN: Thanks. Joy.

MS. PRITTS: At first, I was kind of regretting getting the end spot, worrying I wouldn't have anything left to say, but I think it gives me a great opportunity to finish with what we have been using kind of as our public service announcement in some ways in many of the presentations that we give.

Because it's really -- one of the things that we find that's really important is that everybody has a role to play in protecting this information. The government clearly has an important role here in establishing regulations that are both effective and workable for people. The providers and the plans, of course, have their role in protecting the information when it's in their hands and when they're transmitting it. And then the vendors, the app developers, the device vendors, they are also responsible for building

in privacy and security into their products.

And we could go on with all the other people or the entities that touch this, but it's really a cultural change that we're trying to make here. And it goes all the way down to the patient, because the patient is also responsible. It's going to take a lot of effort from all of us to really bring about this change. I do think that we are kind of at a defining moment here, although we've said that many times over the last several years. But there is a huge movement here with big data and how it's being shared and how all of this information is flowing. And it's really momentous and it's very different than the way things were even ten years ago.

And I think that we are all responsible for sitting back and thinking, how are we going to manage this in a way that's responsible?

MS. HAN: Thanks. So thank you all for coming, I think this is it. A special thank you to our presenters and panelists.

We will be accepting comments on these issues until June 9th and instructions for submitting those comments are available on our event webpage. So thank you again all for coming.

(Whereupon, the proceedings concluded at 12:00 p.m)

C E R T I F I C A T I O N O F R E P O R T E R

MATTER NUMBER: P145401

CASE TITLE: SPRING PRIVACY SERIES

DATE: MAY 7, 2014

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: MARCH 27, 2014

STEPHANIE GILLEY

C E R T I F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

SARA J. VANCE