

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

FEDERAL TRADE COMMISSION
SPRING PRIVACY SERIES
CONSUMER GENERATED AND CONTROLLED
HEALTH DATA

MAY 7, 2014

Federal Trade Commission
601 New Jersey Avenue, N.W., Conference Center
Washington, DC

Reported By: Stephanie Gilley

FEDERAL TRADE COMMISSION

I N D E X

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Session	Page
Welcome	3
Health Data Flows	12
Latanya Sweeney	
A Snapshot of Data Sharing	22
Jah-Juin ("Jared") Ho	
Panel Discussion	29

W E L C O M E

1
2 MS. HAN: Hi, everyone. Good morning and
3 thank you all for joining us for the Spring Privacy
4 seminar, the last in the series of three the FTC has
5 held to explore how emerging practices and technologies
6 are impacting consumer privacy.

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

11 But before we get to that, there are a few
12 housekeeping measures that I've got to get through.
13 First, anyone who goes outside the building without an
14 FTC badge will be required to go through the
15 magnetometer and x-ray machine prior to reentering the
16 conference center.

17 In the event of a fire or evacuation of the
18 building, please leave the building in an orderly
19 fashion. Once outside of the building, you need to
20 orient yourself to New Jersey Avenue. Across from the
21 FTC is the Georgetown Law Center. You'll look to the
22 right front sidewalk, that's going to be our rallying
23 point. Everyone will rally by floors and you'll need
24 to check-in with the person accounting for everyone in
25 the conference center.

1 In the event that it is safer to remain
2 inside, you'll be told where to go inside the building.

3 If you spot suspicious activity, please alert
4 security.

5 This event may be photographed, videotaped,
6 webcast, or otherwise recorded. By participating in
7 this event, you are agreeing that your image and
8 anything you say or submit may be posted indefinitely
9 at FTC.gov or one of the Commission's
10 publically-available social media sites.

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

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

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

25 COMMISSIONER BRILL: Thanks, Cora. I want to

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

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

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

14 Big picture, consumer-generated health
15 information is proliferating. Not just on the web, but
16 also, of course, with respect to connected devices, the
17 internet of things, or as Cisco says so famously on all
18 the TV shows that I watch, the internet of everything.
19 The potential benefits to consumers are significant.
20 The potential benefits to society are incredibly
21 significant. But also, there are some risks, I
22 believe, and I hope we will talk about today, with
23 respect to health data flows that are appearing outside
24 of HIPAA, outside of the medical context, and therefore
25 outside of any regulatory regime that focuses

1 specifically on health information.

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

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

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

25 Or an interesting ethical debate underway in

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

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

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

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

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

1 insurers.

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

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

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

1 for its beneficiaries to use where it will allow their
2 consumers to set goals, track their progress, on all
3 sorts of health indicators. You know, weight,
4 exercise, things like that.

5 Now it's wonderful that Aetna set this up, I
6 think it's great, but I don't know precisely what
7 they're doing with this information. You know, we've
8 looked at the terms of service, but it just raises
9 interesting questions. To what extent could this
10 information be used for rating purposes? And we all
11 know that, under the FCRA, it ought not to be, but what
12 are the rules of the road here?

13 The other interesting example that I remember
14 reading about recently was an entity called Blue Chip
15 Marketing, which was being used by pharmaceutical
16 companies -- or being hired by pharmaceutical companies
17 to help them find candidates for clinical trials.

18 Now Blue Chip Marketing was not a doctor, or
19 didn't work with doctors. It didn't work with
20 hospitals. Instead, it surfed social media, it surfed
21 cable TV subscriptions and got lots of information that
22 allowed it to infer whether consumers were obese,
23 potentially had diabetes, potentially had other medical
24 conditions, and then offered to them to join a clinical
25 trial.

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

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

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

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

25 Thanks.

1 MS. HAN: Thanks Commissioner Brill. To
2 begin the program today, we're going to start off with a
3 presentation by FTC Chief Technologist Latanya Sweeney
4 on health data flows.

5 Let's welcome Latanya.

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 PRESENTATION ONE: HEALTH DATA FLOWS

2 MS. SWEENEY: It's great to be here. And I,
3 too, want to thank Maneesha, Cora, and Kristen for
4 having me and giving me this opportunity to speak.

5 There's a kind of duality in this talk. I
6 absolutely love being at the FTC, but most of you know
7 that my real job, in a sense, is at Harvard, a
8 Professor, so the work I'm going to talk about is
9 actually not work done at the FTC, but it certainly has
10 some intersection points with respect to this workshop.

11 So for that reason, I have to start out with
12 a disclaimer that anything that I say is not the views
13 of the Commissioners or of the Commission and I also
14 have to tell you they are also not officially my views.

15 So I want to talk about the relationship
16 between transparency and trust. Individuals -- as
17 Commissioner Brill made such a great point of talking
18 about the fact that individuals have control of their
19 own data. The data that they can generate, the data
20 that they might pull out of the HIPAA system, in terms
21 of asking for that data from their physician and so
22 forth, and what they can do about it is up to them.
23 And one of the things we all want is for them to live
24 their lives better with that data.

25 The question that gets posed from the kind of

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

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

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

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

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

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

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

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

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

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

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

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

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

1 room? Okay, so that's about half.

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

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

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

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

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

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

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

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

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

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

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

1 story there.

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

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

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

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

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

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

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

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

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

12 Thank you.

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

18

19

20

21

22

23

24

25

1 PRESENTATION TWO: A SNAPSHOT OF DATA SHARING

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

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

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

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

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

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

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

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

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

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

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

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

1 So, a few limitations. We limited our
2 snapshot to one mobile device and therefore one
3 operating system. Our snapshot was limited to free
4 apps, so we did not test any paid apps or if an app had
5 premium features, we didn't purchase those features.

6 We only examined the data transmissions
7 between the apps and the third parties on the
8 front-end, meaning while we were interacting with the
9 app. While additional information collection and
10 sharing can certainly happen on the back-end, our
11 snapshot wouldn't have captured that. And again, we
12 did not review any privacy policies, so we don't make
13 or express any opinions as to the actual information
14 collection practices or sharing practices of the apps
15 themselves or the third parties.

16 So on to the snapshot. We started with 12
17 different apps. During our testing, we found that
18 these 12 apps transmitted information to their
19 developer websites, which are represented here by the
20 yellow dots. Our testing also found that additional
21 information was transmitted to 76 third parties. They
22 are represented here by the blue dots.

23 So what does this graphic mean? Zooming in
24 and taking a closer look at one app as an example, we
25 see that this app transmitted information to 18

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

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

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

1 information about our device.

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

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

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

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

25 And finally, a summary of our observations.

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

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

14

15

16

17

18

19

20

21

22

23

24

25

1 PANEL DISCUSSION

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

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

9 So our discussion this morning will focus on
10 ways in which consumers are generating and managing
11 their own health data. We'll hear from our
12 distinguished panel of experts who all have different
13 perspectives and varied experiences about how consumers
14 are going about this, what some of the risks and
15 benefits are, and what they think the next steps should
16 be to encourage innovation while protecting consumers'
17 privacy.

18 So we're joined today by Dr. Christopher
19 Burrow, who joined the Humetrix executive team in 2010
20 and is the company's principal data security and
21 privacy officer. He is a physician, scientist, and
22 biotechnology executive entrepreneur in the field of
23 genomics and personalized medicine. As a clinician and
24 health information data specialist, Dr. Burrow has
25 played a key role in the development of Humetrix Blue

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

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

12 Next, we have Joseph Lorenzo Hall, who is the
13 Chief Technologist at the Center for Democracy and
14 Technology. His work focuses on the nexus between
15 technology, law and policy, ensuring that technology
16 and technical considerations are appropriately embedded
17 into legal and policy environments.

18 And finally, we have Joy Pritts, who joined
19 the Office of the National Coordinator for Health
20 Information Technology in the Department of Health and
21 Human Services in February of 2010 as its first Chief
22 Privacy Officer. Ms. Pritts provides critical advice
23 to the secretary and national coordinator in developing
24 and implementing ONC's privacy and security programs
25 under HITECH.

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

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

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

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

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

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

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

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

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

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

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

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

25 So for example, in that map, Latanya had an

1 arrow that went to lawyers. Well now, if lawyers are
2 performing a service on behalf of a doctor, for
3 example, then they must also follow HIPAA, the HIPAA
4 rules for privacy and security.

5 On the other hand, if a lawyer subpoenas
6 those documents for another purpose, it is not
7 protected by HIPAA. So you can see that it's a little
8 complicated for people, and particularly laypeople, to
9 understand how this works. Because whether information
10 is protected often depends on -- how the information is
11 protected depends on who is holding it and for what
12 purpose.

13 Does that --

14 MS. HAN: Yeah, that's great. So could you
15 describe like a situation, for example, in which a
16 consumer might unwittingly cause HIPAA-protected data
17 to sort of move outside of the HIPAA bubble?

18 MS. PRITTS: Well, we're actually trying to
19 encourage them to do that, so it's a very -- it's a
20 very interesting situation.

21 So one of the rights that individuals have
22 under the HIPAA Privacy Rule is the right to get a copy
23 of -- the right to get access to their own health
24 information. And that includes getting a copy of that
25 information.

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

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

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

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

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

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

18 MS. HAN: Thanks, Joy.

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

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

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

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

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

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

1 maybe dedicated to diabetes, where a lot of information
2 can be pulled in from -- an app, for example, or a mobile
3 device and it could actually create a profile
4 about you individually.

5 There's others that are really more around
6 support. I'm thinking about, I have this condition,
7 you have this condition, let's try to find ways of
8 being able to share what we know and then find some
9 ways of supporting each other.

10 And then there are apps like PatientsLikeMe,
11 which I'll give you just a brief overview of that, it's
12 really more of a research-based concept on our platform
13 where we actually are helping patients create health
14 profiles using quantified survey-type tools where they
15 are able to create information and then longitudinally
16 track that over time. It happens to be built upon a
17 social network, so the concept being that patients
18 actually have the opportunity not only to create their
19 own personal record, but also to share that and be
20 transparent about that with other people like
21 themselves.

22 I think the other piece that I want to
23 mention about PHR, personal health records, is one area
24 that has not necessarily taken off is the fact that
25 personal health records are actually rather boring,

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

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

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

23 MR. HALL: Sure.

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

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

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

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

25 And finally, there are really innovative

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

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

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

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

1 have a right to electronic data.

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

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

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

25 And as you can see here, this particular

1 patient, I think I have the pointer, this particular
2 patient has several records. This patient has a
3 Medicare record, has a record that he has obtained from
4 TRICARE, which is the -- TRICARE Online is the online
5 site where active duty soldiers and their families can
6 go get an online Blue Button record or their summary
7 record. As well, this particular fictional patient has
8 acquired data from an EMR system called Epic at the
9 University of California, San Diego. And all of these
10 records are captured in the app, where they are stored
11 locally on the device, and the system allows you to
12 create a summary record, that is your medications,
13 immunizations, allergies, and conditions that are
14 extracted from all of those records.

15 Now, there are several ways to get data into
16 this app. And by the way, all of the data is stored
17 locally on the device. There is no silo, there is no
18 cloud. Everything is local on the device, where the
19 data is kept safely encrypted. Any document that you
20 might have on your desktop you can upload into our app.
21 Or you can use the camera function in the app, if
22 you've burned your hand, to take a picture of the burn
23 every day and you might want to share that with your
24 physician when you see them, or if you have other skin
25 lesions, so that they can follow the course of what's

1 happened.

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

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

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

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

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

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

1 service to our users.

2 The new way to get data, you've heard about
3 downloading data from the Medicare Blue Button or VA,
4 the new standards have been put in place called the
5 Blue Button+ standards, require that hospital
6 information systems use something called Direct, which
7 is a secure email protocol to send a defined machine a
8 readable summary of your encounter or your hospital
9 discharge to you to an email address. Our app provides
10 you with that secure address and the physician or
11 physician extender or nurse practitioner can send the
12 record directly to your app. Our app will download it,
13 let you view it, and let you assimilate it with other
14 records that you have to create that summary record.

15 Here's an example. There's the Medicare
16 record on the left, showing all the diagnoses and all
17 the medications. You can scroll down and see all of
18 the ER visits and imaging studies. The next record is
19 an Epic EMR system record from the University of
20 California San Diego. Just to show you, you can view
21 it. The next record is from the VA and then the last
22 display over there, the summary record, is what I was
23 telling you about, where the app has now gone and
24 retrieved, if you will, by parsing through all of the
25 data and the other records, all of the medications that

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 MR. HALL: Okay.

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

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

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

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

16 But anyway, the top concerns for people they
17 studied using Fitbit, and you know it's pretty benign
18 information. To some extent, how many steps you walked
19 from an altimeter sense and then your actual motions
20 translated into how far you've walked, but the things
21 that people cared about were -- the top three were
22 embarrassment, physical safety and the implications for
23 employment and shareability.

24 So in terms of embarrassment, you know Fitbit
25 has a great case study itself where they were

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

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

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

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

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

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

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

1 MS. HAN: Chris.

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

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

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

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

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

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

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

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

13 The Department of Commerce has something that
14 touches on this, which is the NTIA Mobile App
15 Transparency Code of Conduct. And I know there's
16 people in the room that have been there with me,
17 hammering that out, and it actually requires very
18 clear, short form disclosure trying to get at the
19 transparency issues for collections of biometrics and
20 health, medical, and/or therapy information.

21 And finally, the Digital Advertising Alliance
22 and the Network Advertising Initiative are the two main
23 advertising guideline bodies, I guess is the way to say
24 it, have mobile behavioral advertising guidelines that
25 apply to sensitive health information and require a

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

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

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

13 MS. OKUN: I would just add that, you know,
14 consumers themselves, when they are starting to use
15 some of the features that might be available to them on
16 our site, for example, I think Latanya had mentioned,
17 you know, transparency establishes trust. And one of
18 the things we recognized early on, in creating
19 PatientsLikeMe, was that we needed to establish the
20 trust of the patients who were going to be using the
21 site in such a way that we held that as one of our very
22 core -- highest core values. Without it, we really
23 don't have a site.

24 So we pay a lot of attention to our user
25 agreement, to our transparency and openness policies,

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

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

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

1 reasons.

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

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

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

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

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

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

14 MS. HAN: Thanks.

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

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

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

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

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

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

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

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

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

23 MS. OKUN: Mm-hmm.

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

1 MS. OKUN: Sure. The study was actually done
2 as a follow-up study to one that was done by Consumer
3 Reports. It actually had just a couple of questions in
4 it that related to health data sharing that peaked our
5 interest at PatientsLikeMe. And the questions had to
6 do with, would you be willing to share your health data
7 if it were to improve your care or the care of other
8 people like you? And nearly 90 percent of -- a
9 nationally representative sample, within the country,
10 agreed that they would be willing to do that.

11 Now, when asked whether or not they thought
12 it was happening, most people either didn't know or
13 said no. So there's sort of the sense that, you know,
14 I'd be willing to do this, but I'm not sure if it's
15 being done. And if it is being done, then maybe I need
16 to know more about how that works. And I think that
17 speaks to Joy.

18 So we actually learned quite a bit. And what
19 we decided to do is take that question and then expand
20 upon it within our population of chronically ill
21 people. So we actually were able to sort of tease out
22 a little bit. We know the patients on PatientsLikeMe
23 are already sharing their data, so it wasn't surprising
24 to learn that 98 percent of them were willing to share
25 their data if it was going to benefit themselves or

1 someone else.

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

9 Certainly, we've heard some already. Seventy-six
10 percent of the patients interviewed thought that their
11 data could be used without their knowledge. So we
12 already know that it is being used without their
13 knowledge, it's moving on to different places. So that
14 actually validates that concern. Seventy-two percent were
15 concerned about their benefits and being denied
16 benefits. Now, whether we re-asked that question today,
17 in the light of more health coverage, that might be an
18 interesting finding. This was about two years ago that
19 we did the survey. And then 66 percent really were
20 worried about limiting job opportunities.

21 So there's real clear reasons why people
22 would be a little reticent to consider having their
23 payer learn a lot more about their health data, whether
24 or not their employer, again, tied often times to
25 payers, might be learning about this information. So

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

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

12 So their health care provider, 19 percent
13 said they were sharing it with them. Now we found that
14 interesting because -- and we haven't teased it out.
15 Chris and I were talking about this before. We know
16 that some of our patients are bringing their data to
17 their clinicians, only to be rejected. You know, to
18 have them say, I don't know what to do with this
19 information, so I'm not so sure. Let's not even go
20 there.

21 Some of the conditions, when we looked at
22 more specifically where that kind of information is
23 being used at the point of care, is in the mood
24 conditions and psychiatric conditions, where therapists
25 and patients are using this data quite effectively to

1 monitor moods and things like that.

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

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

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

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

8 MS. HAN: Chris.

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

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

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

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

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

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

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

18 MS. HAN: Sure.

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

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

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

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

23 MS. ANDERSON: Thank you.

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

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

1 Patterson hat on and -- Heather, in working as a post
2 doc with Helen Nissenbaum at NYU, has done a study of
3 Fitbit users. And part of what they're trying to
4 figure out is what do Fitbit users think they know about what
5 Fitbit is doing, what are their concerns about the
6 possible future of Fitbit's business model, and I'm
7 sorry that I have to talk so much about a brand, but
8 it's because the study is about a specific user
9 community around a specific brand, and then what kind
10 of data management practices do people employ to manage
11 that kind of uncertainty.

12 The one thing that is interesting is that
13 people have no clue how Fitbit is a business.
14 You know, is it selling the device, is it doing other
15 things with data? They just don't know. And to manage
16 that uncertainty, they employ a whole bunch of really
17 interesting tactics.

18 For example, people don't sign up without
19 using their real name because it's hard for people to,
20 you know, it's a social challenge -- you know, I run
21 or walk farther than you kind of thing. So there's an
22 important role in having your real name involved with
23 that.

24 But people will only share with folks that
25 they've met in real life often, or they'll only share

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

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

16 And so there's a whole bunch of interesting
17 sort of social-management practices that are sort of
18 appearing and evolving with the uses of the wellness
19 devices. And I think we'll see those, too, with health
20 and with specific medical interactions.

21 MS. HAN: Thanks.

22 MS. ANDERSON: Thank you. So one of the
23 other significant privacy issues that we've heard a lot
24 about is transparency, specifically notice and choice.
25 What are some of the challenges to providing effective

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

5 Joe, would you like to start us off?

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

14 But at the same time, if you're expecting
15 people to read 30 pages of legalese and understand it
16 and be fully informed, you're going to have a bad time
17 actually communicating with people about what you're
18 doing, but that's why there are a bunch of other
19 efforts. So for example, there are some platforms, like
20 Apple's iOS platform that use just-in-time
21 notification. So if this app is trying to access your
22 location data, yea or nay. And if you say nay, then
23 it's not going to get that. If that's a mapping app,
24 that app may have very little functionality after you
25 deny where you are. Or I may not just be able to do

1 things like directions and stuff like that.

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

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

1 a summary of your clinical interaction. And then the
2 app can say, this app is trying to access your medical
3 records or is trying to store something of a health
4 data-nature to you. And if those guidelines were
5 enforced by app stores, that can be a really neat thing
6 and can allow people to have sort of some of the things
7 that Humetrix and iBlueButton do in this very
8 controlled sort of environment, but make that available
9 on a more platform and more generic way.

10 DR. BURROW: Well, certainly we started four
11 years ago to build an app that was highly secure, all
12 native, you control your own data. We also built in
13 privacy warnings.

14 For example, even though the data transfer to
15 the provider's iPad is completely secure and uses a
16 one-time cryptographic key, is resistant to all manner
17 of attack, there is no data persistence, we still put
18 up a little warning saying, you are about to send your
19 health data to your -- to this person with an iPad. Be
20 sure it's, you know, the right physician and you both
21 authenticate each other and look at each other. So we
22 think that's great.

23 With regard to the ONC's Model Privacy Notice,
24 we think that's a step in the right direction. It's
25 what Joe referred to as the soup can label idea. I'm

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

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

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

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

15 MS. ANDERSON: Right.

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

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

23 So you might have a soup label type of notice
24 up front, but then back-end use. And we've heard a
25 little bit about that in the presentations and some of

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

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

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

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

1 we have.

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

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

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

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

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

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

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

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

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

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

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

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

9 I also think, when you hear this
10 conversation, it's like, well, only 10 percent of the
11 people in America really care about privacy. But that
12 10 or 20 percent is flexible. It's not a static
13 number. People come and they flow into and out of, you
14 know, how much and whether they care about how they're
15 sharing their information, depending on, again, the
16 context.

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

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

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

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

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

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

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

1 available outside of the sphere that they expected it
2 to be used in. But at the same time, each of us as
3 consumers are going to need to expand our awareness and
4 understanding, what can we do personally, since we will
5 be given a lot more responsibility to have access to
6 our medical information that we previously have not had
7 available to us, as well as begin to share that in
8 places that maybe are not as protected as we might
9 think they are.

10 DR. BURROW: And I'd also make the point,
11 and the Commissioner made this point earlier today,
12 we've spent a lot of time talking about the costs and
13 the risk of privacy, and those are all very real and
14 digging deep, but the benefit can be extraordinary to
15 having these kinds of technologies available.

16 You don't necessarily have to understand your
17 record. I'm not trying, with the iBlueButton app, to
18 make all of you physicians or specialists as
19 physicians, but I am trying to give you the basic
20 building blocks so that that data will be available
21 when you go somewhere else and see another physician.

22 And so that's really -- I think there is
23 enormous benefit. And I don't have time to go into all
24 of the studies that have showed that just having a
25 medication list that's up-to-date and a condition list

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

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

8 DR. BURROW: Yeah.

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

12 And first there was a question from the
13 audience. So there's talk, and this is what we've been
14 discussing a few times, about sharing data in
15 de-identified form. So could people comment on
16 Latanya's finding that her group was able to reidentify
17 43 percent of the sample? And would consumers
18 appreciate this and how should policy makers account
19 for consumers not being able to understand? So there's
20 a lot there, but I think --

21 DR. BURROW: Well, I'll jump in and make the
22 first obvious comment, although it may not be obvious
23 to all of the people in the room. In the HIPAA
24 guidance on data de-identification, it states very
25 clearly that gender, five digit zip code, and date of

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

5 MR. HALL: I was just going to make one
6 slight correction, which is Latanya's original study
7 showed a higher number than that. I think it was
8 70-something and then there was a follow-up using the
9 2000 census data by Philippe Golle, which dropped that
10 down to like 60-something, so it's big.

11 MS. HAN: Thanks.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6 MS. HAN: Others?

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

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

25 And you also want to think about the threats,

1 the threats to re-identification that might exist,
2 depending on what you're going to do. And if you're
3 going to post stuff online publicly, you're going to
4 have a severe -- a very large sort of threat surface.

5 You know, just the last point is that, making
6 a sort of global comment, there was a really neat paper
7 issued from something from Europe called the Article 29
8 Working Party, which was on basically anonymization and
9 techniques for doing anonymization, so a little
10 stronger than even de-identification.

11 And they had a whole bunch of really neat
12 sort of like walking you through how to do certain
13 things. Like if this is what you want to do with the
14 data, you can shuffle these whole columns and you're
15 not going to ruin the statistical information in there,
16 but you're not going to be able to -- if someone does
17 end up reidentifying that row, they won't really have
18 much confidence in the individual that was
19 reidentified, too, because it's a mix of a bunch of
20 people's stuff. But you have to be very careful in how
21 you do that.

22 And so an effort to do a standard may be
23 really interesting, I just wonder if it wouldn't boil
24 down to, you know, a few clear-cut cases with some more
25 generic case-by-case kind of guidance.

1 And I'm also a big fan of the version of the HIPAA
2 de-identification that isn't, remove these 19
3 identifying kinds of quantities, but you know, engage
4 with an expert to actually probabilistically determine,
5 given your use, to what extent these might be
6 re-identifiable. That's a little hard, and expensive,
7 because you have to engage with an expert and there's
8 not a lot of people who do that. You go to try to find
9 more than two or three of them and it gets pretty
10 difficult pretty quick. And we try to do that when
11 people ask us, how do we do this well, and it turns out
12 to be a few people that are overwhelmed and such.

13 DR. BURROW: Well, I think we need to get
14 beyond the standard privacy policy. We share your --
15 unless you opt-in, we won't share. If you do opt-in,
16 we will share your personal information, but it will be
17 de-identified. But the next sentence should be, we're
18 sharing it with -- could be, we're sharing it with a
19 large, extremely competent, sophisticated data
20 analytics shop that is running big data that will
21 probably be able to reidentify most of your data. But
22 you know, that's a different statement. So there's a
23 sentence missing.

24 And just the long way of answering this
25 question, I think we do need to move towards more

1 transparency on this issue.

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

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

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

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

4 DR. BURROW: Certainly, there are core
5 things that we all agree are health care data. Your
6 names of your medications, the names of your medical
7 conditions, your allergies, the immunizations you've
8 had, the treatments you've had, the surgeries you've
9 had. I mean, I think we can all agree on -- in that
10 inner circle, we can agree on a lot.

11 Now I agree, as you get larger and larger
12 circles, you start to get disparities in what people
13 think of as health data, so that's where the trouble
14 starts.

15 But to keep it simple, we can also focus on
16 this inner circle of data that we can all agree about
17 as health data, with regard to policy.

18 MS. OKUN: The only problem I would suggest
19 with that is that we then lose the nuance of the
20 context of the human element of what health is. So I
21 would say that that would give us a narrow picture,
22 probably a provider or clinician-centric picture.

23 DR. BURROW: Right.

24 MS. OKUN: And so we just need to be careful
25 about that.

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

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

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

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

25 But there were things that they found really

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

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

25 MS. ANDERSON: Thanks.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 MS. HAN: Thank you, Sally. Joe.

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

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

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

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

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

9 MS. HAN: Thanks. Joy.

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

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

1 in privacy and security into their products.

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

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

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

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

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

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

2

3 MATTER NUMBER: P145401

4 CASE TITLE: SPRING PRIVACY SERIES

5 DATE: MAY 7, 2014

6

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

11

12

DATED: MARCH 27, 2014

13

14

15

STEPHANIE GILLEY

16

17

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

18

19

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

21

22

23

24

SARA J. VANCE

25