

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
COMPETITION AND CONSUMER PROTECTION
IN THE 21ST CENTURY

Tuesday, April 9, 2019
9:00 a.m.

FTC - Constitution Center
400 7th Street, SW
Washington, DC

1	FEDERAL TRADE COMMISSION	
2	I N D E X	
3		PAGE :
4	Welcome and Introductory Remarks	3
5		
6	Opening Remarks - Joseph J. Simons, Chairman	7
7		
8	Goals of Privacy Protection	13
9		
10	The Data Risk Spectrum: From De-Identified	
11	Data to Sensitive Individually Identifiable	
12	Data	72
13		
14	Remarks - Noah Joshua Phillips, Commissioner	132
15		
16	Consumer Demand and Expectations for Privacy	145
17		
18	Current Approaches to Privacy, Part 1	189
19		
20	Current Approaches to Privacy, Part 2	252
21		
22	Closing Remarks	316
23		
24		
25		

1

WELCOME

2

(9:00 a.m.)

3

MR. TRILLING: Good morning, everyone.

4

Welcome to the Federal Trade Commission and the first

5

day of our hearing on the FTC's Approach to Consumer

6

Privacy. My name is Jim Trilling. I am an attorney

7

in the FTC's Division of Privacy and Identity

8

Protection. Before we get started with the substance

9

of the hearing, I have a number of brief

10

administrative announcements that will apply

11

throughout the hearing.

12

First, if you leave the Constitution Center

13

building during the hearing, you will need to go back

14

through security screening again, so please allocate

15

time for that.

16

Restrooms are located outside of the

17

auditorium, in the hallway, and the Constitution

18

Center building cafeteria is located around the

19

corner on this floor of the building. If an

20

emergency requires you to leave the auditorium but

21

remain in the building, please follow the

22

instructions that will be provided over the

23

building's PA system.

24

If an emergency requires evacuation of the

25

building, an alarm will sound. Please leave the

1 building in an orderly manner through the 7th Street
2 exit. When you get outside, turn left and proceed
3 down 7th Street and across E Street to the FTC
4 emergency assembly area and remain in that area for
5 instructions to return to the building or otherwise.
6 If you notice any suspicious activity, please alert
7 the building security staff.

8 This hearing is being photographed, webcast,
9 and recorded. By participating in the hearing you are
10 agreeing that your image and anything that you say or
11 submit may be posted indefinitely at FTC.gov, on
12 regulations.gov, or on one of the Commission's
13 publicly available social media sites.

14 The webcast recording and transcripts of
15 the hearing will be available on the FTC's website
16 shortly after the hearing concludes. Webcast
17 recordings and transcripts from all of the FTC
18 hearings on competition and consumer protection are
19 available on the FTC website. Audio files from the
20 hearings are available to be streamed or downloaded at
21 FTC.gov/audio.

22 Please silence your cell phones and other
23 devices. We want to make sure that everybody has the
24 ability to be heard. Attempts to address the hearing
25 speakers while this hearing is in progress and other

1 actions that interfere or attempt to interfere with
2 the conduct of this hearing or the audience's ability
3 to observe the hearing are not permitted. Any persons
4 engaging in such behavior will be asked to leave.
5 Anyone who refuses to leave voluntarily will be
6 escorted from the building.

7 During the panels, the audience is invited
8 to submit questions via question cards available
9 from FTC staff and in the hallway outside the
10 auditorium. If you would like to submit a question,
11 please write the question on a card and raise your
12 hand to signal for FTC staff to collect the question
13 from you.

14 FTC Commissioners and staff are unable to
15 accept documents during the hearing. Such documents
16 will not become part of the official record of any
17 Commission proceeding or be considered by the
18 Commission. We do invite the public to submit
19 written comments for the hearing. You can submit
20 comments online via the link on the FTC website
21 until May 31.

22 If you received a visitor's badge today,
23 please return it to the security staff on your way out
24 of the building so that we can reuse it.

25 With those logistics out of the way, we can

1 now move on to the substance of the hearing. I am
2 pleased to turn the podium over to FTC Chairman Joseph
3 Simons for opening remarks.

4 (Applause.)

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

1 Have we become inured to these privacy
2 incidents? Not at all. In the face of these
3 disclosures, consumers report that they do care about
4 their privacy and that they value the ability to
5 control what information is collected about them and
6 who can get that data. These concerns arise from the
7 recognition that privacy violations can cause a range
8 of real harms, including fraudulent charges on credit
9 cards, safety risks, reputational injury, and unwanted
10 intrusion into people's homes and the intimate details
11 of their lives.

12 And, ultimately, that's why we are here
13 today. Together with the public comment process that
14 we started last summer, this hearing marks one of the
15 Commission's most extensive efforts to engage the
16 public on data privacy issues since the Commission
17 issued its comprehensive privacy report in 2012.
18 These hearings are part of a greater effort by the FTC
19 to stay abreast of new and emerging technologies as
20 they rapidly evolve.

21 The FTC has long been the cop on this
22 particular beat. Over the past two decades, we've
23 brought hundreds of cases, conducted over 70
24 workshops, and issued about 50 reports to help protect
25 consumers' privacy. Our work over the last year

1 demonstrates the FTC's approach to consumer privacy,
2 vigorous enforcement with every tool that we have.
3 For example, in February, we announced a settlement
4 that includes the largest civil penalty the Commission
5 has ever obtained under COPPA. Last fall, we obtained
6 a \$3 million civil penalty under FCRA against a
7 company whose automated decision-making tool provided
8 inaccurate data to property managers, resulting in
9 denial of housing.

10 We've used our Section 5 authority to
11 challenge false claims about compliance with the EU/US
12 Privacy Shield and to stop purveyors of fake paystubs
13 that identity thieves used to get jobs and housing in
14 other people's names. We brought privacy cases
15 against a revenge porn site, a mobile phone
16 manufacturer, a peer-to-peer payment service, and an
17 apps-based ride service.

18 We've also filed two advocacy comments,
19 announced five public events, issued a staff report on
20 privacy injuries, and issued a notice of proposed
21 rulemaking to help military personnel get free credit
22 reports. As this list of accomplishments
23 demonstrates, the FTC has done a remarkable job to
24 protect consumers' privacy with the tools and the
25 resources at our disposal. But we must do more. We

1 need to continue evaluating privacy risks as they
2 evolve. What approach will protect consumers' privacy
3 interests while fostering innovation and competition
4 that has brought us so many benefits?

5 That brings us back to the agenda for this
6 hearing. Over the next two days, you will hear from
7 dozens of leading experts from government, academia,
8 business, and policy shops who have thought deeply
9 about these issues. Today, we begin with a
10 conversation about the goals of privacy. What exactly
11 are the harms that we are trying to address, and what
12 are the countervailing considerations, like the effect
13 on innovation and competition?

14 We will then turn to the data risk spectrum.
15 Panelists will evaluate what makes data sensitive,
16 whether privacy protection should depend on such
17 classifications, and how effective are techniques to
18 de-identify that data.

19 After lunch, we will hear from my colleague,
20 Commissioner Phillips, who will share his thoughts
21 about the Commission's privacy work. We will then
22 discuss consumer demand and expectations for privacy,
23 as well as whether and how companies respond or should
24 respond to such demands.

25 And we will round out today's session with a

1 two-part discussion about current approaches to
2 privacy. Panelists will discuss, compare, and
3 contrast US and international privacy laws and self-
4 regulatory frameworks. As policymakers consider
5 privacy legislation, the panelists will consider what
6 such a law might look like.

7 Tomorrow, we will explore pros and cons of
8 possible frameworks for protecting consumer privacy.
9 The first panel will examine the role of notice and
10 choice. Panelists will explore the various roles that
11 notice and choice play in the current marketplace as
12 well as consider limitations on the effectiveness of
13 notice and choice and offer ideas for addressing them.

14 The second panel will analyze the role of
15 access, deletion, and correction. Panelists will
16 address the costs and benefits of providing these
17 types of tools and will share their experience of how
18 consumers use them.

19 Commissioner Slaughter will provide her
20 views about the FTC's privacy work, and then a panel
21 will share views about what makes firms accountable
22 for their privacy practices and whether policymakers
23 should attempt to improve accountability from within
24 organizations.

25 Finally, two sets of panelists will discuss

1 whether the FTC has an adequate toolkit for protecting
2 consumer privacy, covering topics such as the use of
3 our existing authorities, as well as the need for new
4 resources.

5 We are excited to get this discussion
6 started, but, first, I want to thank the 50 panelists
7 for participating in this event. We greatly
8 appreciate your willingness to share your insights and
9 your expertise. And I want to thank Jim Trilling, who
10 you saw up here moments ago; his colleagues, Elisa
11 Jillson and Jared Ho, for leading the planning of this
12 hearing; and I also want to thank my many other FTC
13 colleagues from the Division of Privacy and Identity
14 Protection, the Bureau of Consumer Protection more
15 generally, the Bureau of Economics, the Office of
16 Policy Planning, the Office of Public Affairs, and the
17 Office of the Executive Director who have worked so
18 hard together to produce this event.

19 Finally, thank you to everyone who is
20 attending in person or watching online via our live
21 webcast. We appreciate the opportunity to engage the
22 public on this important topic, and I hope you enjoy
23 the hearing. Have a great day.

24 (Applause.)

25

1 GOALS OF PRIVACY PROTECTION

2 MR. COOPER: Welcome. I'm James Cooper.
3 I'm the Deputy Director for Economic Analysis in the
4 Bureau of Consumer Protection. I'm happy to be here
5 to have the first panel to kind of set the stage and
6 bring us up to date to discuss some of the research
7 that we heard about back in the fall on the hearing on
8 privacy, big data, and competition.

9 Let me just give a brief introduction to the
10 panel. I'm going to give kind of a brief
11 presentation, but let me introduce the panel right
12 now. We have Neil Chilson. Neil is the Senior
13 Research Fellow for Technology and Innovation at the
14 Charles Koch Institute. Before that, he was the
15 Acting Chief Technologist under Acting Chairman
16 Maureen Ohlhausen and then an advisor for Acting
17 Chairman Ohlhausen. And before that, he was a
18 telecommunications lawyer at Wilkinson Barker &
19 Knauer.

20 Next to Neil is Alastair Mactaggart.
21 Alastair is the Chairman of Californians for Consumer
22 Privacy, and you all probably know him best for his
23 leading role in the passage of California Bill 375,
24 better known as the California Consumer Privacy Act.

25 And, finally, next to Alastair is Paul Ohm.

1 Paul is Professor of Law and the Associate Dean for
2 Academic Affairs at Georgetown University Law Center.
3 Paul is a leading scholar in information privacy,
4 computer crime, intellectual property. All things
5 digital really, that's Paul. And, also, he did a
6 stint here at the FTC a few years ago as a senior
7 policy advisor working on these very issues.

8 So we have a great panel to discuss what
9 Chairman Simons said, the goals of privacy protection.
10 As we think through the issues on how best to protect
11 privacy for consumers, it's important to maybe go back
12 to some first principles and think about how that --
13 to weigh, as Chairman Simons says, think about the
14 benefits, what are we trying to do and, at the same
15 time think about some of the risks. So there we go.

16 So when we think about, really, any
17 regulation, any type of government intervention, we
18 should ask a couple of questions. The first is what
19 do consumers want. What is it that -- what are their
20 demands? The second thing, and I'm saying this as an
21 economist -- and I'm putting my economist hat on --
22 the second thing that we should be interested in is,
23 well, if there's something that consumers want, if
24 there's a market, if there's some transaction that
25 should be occurring, is it happening, is the market

1 able to mediate these demands, often referred to as a
2 market failure? And that's bad for society. If
3 there's a market failure, that means that there is
4 some kind of welfare-increasing transaction that is
5 not occurring.

6 So the third question we should ask is,
7 well, if that's the case, is there something that
8 government could do, is there some sort of
9 intervention that can make things better. Now, a
10 market failure is a necessary condition, but it's not
11 necessarily a sufficient condition because, again, as
12 Chairman Simons discussed in his opening remarks,
13 there are often risks and countervailing costs that
14 come with any intervention, and those always need to
15 be considered.

16 So moving from the more -- from the general
17 to the specific, let's drill down a little bit and
18 talk about privacy -- apply some of this framework to
19 privacy. Okay, first, what do consumers want? Well,
20 survey evidence suggests that privacy is very
21 important to consumers. You see that in Pew polls,
22 you see that in really popular press. Consumers
23 really do care about their privacy. It's expressed a
24 lot.

25 But we also see revealed preference, which

1 is when actual trades are made in the marketplace,
2 when actual decisions are made, that there is a lot of
3 evidence, both experimental and in the real world, to
4 suggest that, well, consumers are willing to trade
5 information about themselves for a very small amount.
6 This has given rise -- this is what is referred to in
7 the privacy literature as the privacy paradox, and
8 it's something, at least in the academic world, that
9 we try to square. It is a paradox. Why do we see on
10 one hand that privacy is clearly something that people
11 care deeply about, but, in the real world, they seem
12 to make different trades?

13 So the next question is, is there some kind
14 of market failure? Are consumers really getting the
15 type of privacy protections that they want? So we
16 said that revealed preference suggests that the
17 consumers are willing to trade information for small
18 amounts of money or convenience or access to content.
19 Well, what revealed preference will -- a market
20 outcome will correctly show consumer preferences, but
21 markets don't always work. There could be failures
22 like asymmetric information. The data ecosystem is
23 notoriously complex, do consumers really understand
24 what's going on? Behind the scene, there are also
25 cognitive biases.

1 Alessandro Acquisti and a lot of his
2 colleagues at Carnegie Mellon have done a lot of work
3 in this area, but we all know that consumers from the
4 behavioral economics literature suffer a variety of
5 systematic errors, especially in being able to assess
6 long-term benefits and cost. So we have those -- we
7 look at that.

8 There's also market power. Maybe market
9 power can sometimes be thought of as a market failure,
10 depending on how a firm gained that market power. On
11 the other side of that, when we're asking whether
12 there's a market failure, understanding is endogenous
13 in the sense that what concept and economics called
14 rational ignorance, that gathering information is
15 costly, and rational individuals will gather
16 information up to the point where the marginal benefit
17 of that information is equal to the marginal cost.

18 When we go out into the marketplace all the
19 time, we don't always have perfect information of the
20 distribution and prices, and I think we could all
21 think about times where we've gone and bought
22 something and found out, oh, I don't really like this
23 or I could have gotten it cheaper somewhere else, but
24 that's rational, it's rational ignorance.

25 We also know that there is a powerful

1 incentive for firms to reveal good things about them
2 relative to their competitors. It's this unraveling
3 principle that if I can credibly show you that I, say,
4 provide more privacy than my competing firms, then I
5 have a really, really strong incentive to do that
6 because I'll gather more customers.

7 Also, we see in the context of behavioral
8 economics that, as stakes increase, there's at least
9 experimental literature to suggest that, as stakes
10 increase, consumers tend to -- the biases tend to wash
11 out or become a little less pronounced. So it's
12 unclear, when we think about -- when we think about
13 whether there's a market failure, there is evidence on
14 both sides of this.

15 And, finally, when we think about -- we
16 think about intervention, what should government do?
17 Well, certainly the clear benefit from any privacy
18 regulation is, if there is a market failure, if
19 consumers really want a certain level of privacy and
20 control over their information and it is not being
21 provided to them, government intervention will help
22 mediate that demand.

23 So if the market isn't mediating the demand
24 for control over information, well, government
25 intervention can provide that and increase welfare.

1 At the same time, there are costs -- there's a large
2 literature, both empirical and theoretical, that
3 retarding information flows can have negative impacts
4 on market performance and innovation, and we'll talk
5 in a second about some of the research that was
6 presented back in the fall at the hearings.

7 And, finally, when we think about what
8 government should do, the form of intervention
9 matters. Do we want to have an enforcement regime
10 where we go after identifiable harms with law
11 enforcement, take people to court, kind of in the way
12 that the FTC acts now? There's ex ante regulation in
13 the sense of commanding ahead of time what firms need
14 to do. There's the FIPPs model. There are lots of
15 different regulatory models, and so the form that it
16 takes really can have an impact on government
17 intervention.

18 So taking that framework and now moving --
19 I want to go back to the fall and think of this as
20 maybe the last episode of the FTC privacy hearings,
21 just as a recap to bring you up to date, to inform
22 some of these questions that we need to think about
23 when we think about the goals of privacy protection.
24 So what have we heard? We heard, again, going to
25 privacy paradox that even with full information we

1 have experimental evidence showing that consumers
2 choose to reveal private information for very little
3 compensation.

4 We're heard some work both from Lior
5 Strahilevitz and Omri Ben-Shahar some experimental
6 work that they've done. At the same time, we also
7 heard work -- we heard about work from Alessandro
8 Acquisti and some of his coauthors and Catherine
9 Tucker and Amalia Miller that increasing trust can
10 increase the willingness to share data that suggests
11 that a lack of privacy protection, perhaps even in the
12 healthcare area, can have some chilling effects. So
13 we found out that when you give consumers control over
14 the sharing of their data in genetic testing, that it
15 suggests that it increases the willingness to engage
16 in genetic testing.

17 We also heard about research that increases
18 in level that health information exchanges tend to
19 perform better or tend to -- there tend to be more
20 health information exchanges when there are consent
21 requirements coupled with financial incentives. So
22 what else have we heard?

23 We think about the costs and often privacy
24 regulation. We think of opt-in versus opt-out. One
25 of the big areas of potential costs is the revenue

1 generated from targeted advertising. So what do we
2 find? Well, a lot of research, we had a lot of
3 experts at that hearing, a lot of people who are
4 expert on the online advertising ecosystem, and we
5 heard that behavioral targeting tends to generate more
6 revenue for content providers than contextual
7 advertising. There seems to be a lot of empirical
8 evidence to suggest that, but there needs to be some
9 caution.

10 First of all, there are strong selection
11 effects, meaning it's really hard to distinguish
12 between who gets to see a targeted ad, well, someone
13 who probably already expressed an intention to buy
14 that product. How do you distinguish between the
15 effect of the ad or the fact that this person already
16 had expressed a lot of interest in buying the product,
17 would they have bought it anyway? These are what are
18 called selection effects. The ads are selected to
19 people who are more willing to buy the product. So
20 it's hard to figure that out.

21 We saw that there is increased revenue
22 to content providers from targeting, but it tends to
23 be larger than the correctly measured lift to
24 advertisers. Again, it goes to maybe this difficulty
25 in measuring lift. We also heard interesting work

1 from Catherine Tucker that suggested despite the idea
2 that AI and big data algorithms know everything about
3 us and are able to predict with just scary accuracy
4 that, in fact, she unpacked some of these algorithms
5 and found that they weren't -- they were worse than
6 chance at predicting gender, for instance, that there
7 are a lot of -- that maybe the targeting and maybe the
8 fears of AI, the privacy fears aren't that much. And,
9 also, the flip side of that is the extent to which
10 opt-in versus opt-out is going to have a big impact on
11 revenue, maybe we need to investigate that more
12 carefully.

13 So, finally, the other thing, the last -- I
14 didn't want to miss that last bullet point there. We
15 heard some evidence from Liad Wagman on how opt-in at
16 the same time reduces the quality of matching and data
17 collection. This is in loan data using experiments
18 from the San Francisco area where locality used on
19 opt-in versus GOB opt-out and found that the quality
20 of data, when you can't sell it downstream, turns out
21 to be lower and was associated with larger
22 foreclosures.

23 Finally, again, more evidence from Liad
24 Wagman, as well as Ginger Jin, Former Director of the
25 Bureau of Economics, saw that looking at the impact of

1 GDPR on VC investments, some interesting -- at least
2 this is early-phase research and looking at the short
3 run, is that there was a negative impact, somewhere
4 between 27 and 56 percent in value, for European
5 startups versus their counterparts in the US using
6 good treatment and control methods. We also heard
7 about work from Catherine Tucker and Amalia Miller
8 about the negative impact in HIT investments and on
9 health outcomes.

10 Finally, we heard a lot of theoretical
11 papers that suggest that privacy regulation can have a
12 negative impact on competition, primarily by softening
13 competition to the extent that firms are able to
14 gather data to more precisely target consumers, they
15 can become more effective competitors. If you prevent
16 that from happening or make that more difficult, you
17 may have less intense competition.

18 There is also the notion that bigger firms
19 are more able to deal with regulation than smaller
20 firms. However, these results are sensitive both to
21 consumer preferences for privacy and on market
22 structure, elasticity of demand parameters in the
23 model. And, again, it's theoretical work. We don't
24 really -- we didn't really have any empirical work on
25 that.

1 So with bringing us up to date in setting
2 the stage, I'm going to sit down here and begin a
3 discussion with our esteemed panel to drill down on
4 some of these issues as we think about the path
5 forward in protecting -- our goals in protecting
6 privacy protection.

7 All right.

8 MR. CHILSON: Thanks, James.

9 MR. COOPER: You're welcome. So at least
10 one person enjoyed my talk. Thank you.

11 (Laughter.)

12 MR. COOPER: And so you'll get the first
13 question because of that, Neil, the first. So we
14 think about the first part of the question, going back
15 to, you know, what are the problems we're trying to
16 solve. You know, you've thought a lot about this.
17 What do you think of -- what do you think of is --
18 what's the harm that any privacy policy should be
19 directed at? What should we be -- what is the -- what
20 do consumers want and what problems are we trying to
21 solve?

22 MR. CHILSON: Well, I think the first step
23 to answering that question, I'm going to take it back
24 a little bit further, and I think the first step is to
25 define what we mean by privacy, and it's a very

1 complex word. There's a lot of values that people put
2 into the word "privacy." I've been on panels where
3 the discussion has ranged from identity fraud, you
4 know, concerns about identity fraud all the way to
5 misinformation and election manipulation. Those are
6 radically different problems.

7 So what do we mean when we say "privacy"?
8 And I've tried to think about it in a very generic
9 version, like the most abstract version I could think
10 of of what privacy means. And I think this captures
11 many of the definitions of privacy, but I'm sure
12 Alastair and Paul and James will correct me if I've
13 missed one, and that's that privacy is a constraint on
14 somebody else's use of information about you. That
15 constraint can be a physical constraint -- sorry.
16 Privacy is the effect of that constraint. Right?

17 And so that constraint can be a physical
18 constraint or it can be a legal constraint, or it can
19 be a social constraint, or it can be a contractual
20 constraint. So there's lots of different types of
21 constraint. But when I say information, that's a
22 pretty vague term as well. And so there is a
23 scientific definition for information, and I'll rely
24 on that a little bit.

25 And so information is the content of a

1 signal that's going from one party to another. So,
2 for example, the sounds that are coming out of my
3 mouth contain information, they carry information.
4 The light that's reflecting off my body contains
5 information. And because we exist in the physical
6 world and we interact with the physical world, we're
7 constantly generating information, and we can't
8 control -- we can't control all of it. We can try to
9 control certain things and, in the physical world, we
10 understand what the limits of that control are.

11 So I can control the light that's bouncing
12 off my body, or I can attempt to, by wearing clothes,
13 a fact that I assume you all are grateful for. So --
14 but even when I try to constrain information in that
15 way, I am giving off some information about myself,
16 even with that constraint. And so when we think about
17 information that way, it has some implications for
18 privacy.

19 If my goal is to constrain information, it
20 immediately demonstrates that there's two parties
21 involved. There's me and then the party who is
22 presumably going to collect or use the information,
23 probably many other parties as well, and my privacy
24 protections are in tension with that person's use of
25 information about the world, and that we have to draw

1 lines somehow about how we're going to divvy up
2 someone else's ability to observe the world and use
3 that information, sometimes to serve me, sometimes to
4 serve their own purposes, it depends, and my rights --
5 my control, my physical ability, but then also my
6 interests in controlling information.

7 And, so, when we think about it that
8 abstractly, I think it comes down to how do we draw
9 those lines in society? And we tend to focus on harm.
10 When we get government involved, we tend to want to
11 say, we're going to draw those constraints around
12 where one person is injured. And what does injury
13 mean in this case? Now I'm back to your question.

14 MR. COOPER: Finally.

15 MR. CHILSON: Finally, I know. Quite a
16 diversion there. So I want to do this as sort of
17 concentric circles, right? So there are certain harms
18 I think everybody agrees are privacy harms, and those
19 are uses of information that might result in physical
20 injury, financial loss, or increased risks around
21 those two things. I think that those areas, people
22 generally agree that those are the types of things
23 that we might need government intervention to solve.

24 Now, if you get further out from that, there
25 can be disagreements around what other types. And the

1 Chairman mentioned a bunch of different types of harms
2 and some work that Maureen Ohlhausen did in talking
3 about informational injuries, also talked about this.
4 And the types of harms that the FTC has looked at are
5 not just financial harms, are not just, you know,
6 these safety risks or safety injuries, but there are
7 some other harms that are often mentioned in FTC
8 cases. We do have reputational harm. We do have
9 invasion of the home. Now, reputational harm in FTC
10 cases has never been a sole vector for a case, but it
11 is one thing that the FTC has recognized as a
12 potential injury.

13 So basically because of that concentric
14 circle approach, what I want to argue is that we are
15 on the strongest empirical ground of government
16 invention when we are closer to that core, and we get
17 -- it gets less clear that we're doing good for
18 consumers the further we get from that core. And, in
19 fact, we could -- there's some potential that we're
20 actively causing harm, that we're drawing that line
21 between the party who the information is about and the
22 party who is using the information in the wrong place
23 the further we get out.

24 And the reason I think that government
25 intervention is best justified the closer you get to

1 that core is because government's resources are
2 limited, and, so, if we are focusing on less tangible
3 and more -- less objective injuries, and to the cost
4 of focusing on objective, concrete injuries to
5 consumers, we're probably, on balance, leaving
6 consumers worse off. So if we're ignoring some actual
7 harms that we know about, some ones that everybody
8 agrees on, and we're doing other things, we might be
9 making consumers worse off.

10 Second, tangible objective injuries are
11 easier to redress. It can be very difficult to revive
12 somebody's reputation. And the question is how can
13 government do that. This gets to the point that James
14 is making. Sometimes there are things that we should
15 do but we can't do, right? That we want to do but we
16 can't. And that's just a fact of life. And I think
17 that we do ourself a disservice if we pretend like
18 government can do certain things that it cannot
19 achieve.

20 Tangible objective injuries are easier to
21 redress. When we're talking about financial harm and
22 we can put dollar amounts and compensation around
23 physical injury, you can't make somebody perfectly
24 whole, but we have models in the past through tort law
25 that show how we might approach those problems. Other

1 types of injury, it might be harder for government to
2 work on.

3 And, finally, markets are better to solve
4 this -- markets can be better -- can be better -- at
5 solving concerns where there's a multiplicity of
6 perspectives on whether or not there's an injury, and
7 this happens a lot in the privacy space where what is
8 one person's harm is another person's benefit, and in
9 those cases, a government intervention that tries to
10 draw the line between those two and says, well, I'm
11 going to determine that this is a harm and this is a
12 benefit, at that point, you're making one group worse
13 off for the benefit of another group.

14 And so we need to be very careful on that,
15 and that happens less and less the closer you get to
16 that core of physical or financial injury. That's not
17 to say that there aren't other issues that government
18 should play a role in, and it can play a lot of
19 different roles, but we have other tools other than
20 government intervention, and I think a lot of the
21 other panels will talk about that, but that's sort of
22 how I think about harm as the core harms and then as
23 sort of concentric circles that build out from those.
24 And we're safest with government intervention in the
25 center, and we're taking more chances that we're

1 drawing the lines wrong and potentially making
2 consumers worse off the further out we get from that
3 center.

4 MR. COOPER: Thanks. Let me let Alastair
5 and Paul kind of jump in. And we heard Neil say that
6 he's thinking about our threshold question as far as
7 what do consumers want, and Neil would focus this on
8 addressing certain informational harms, maybe a core.
9 What do you all see?

10 And maybe, Paul, I'll throw it to you. I
11 mean, what do you make of -- what do you think
12 consumers want? And how do you -- I know you've
13 thought about the privacy paradox. How do we square
14 that or do you have a way? Can you solve the privacy
15 paradox for us right now?

16 MR. OHM: Yeah, sure. Let me get to that in
17 a few minutes. There's so much I want to say. Thank
18 you to the FTC for having me here. Neil started by
19 saying that he's been thinking about this for a long
20 time, I think he means 120 years, because the
21 presentation that he made, I think, reflects a kind of
22 antiquated crab notion about privacy and harm.

23 And I think if our role as first panelists
24 to is exhort the FTC, which has been a phenomenal
25 leader in this space but is at a crossroads where

1 increasingly politicians, people with power, and
2 average citizens seem like everything is going to hell
3 in a handbasket, to use the technical phrase, online,
4 I think it's really incumbent on the FTC to think
5 hard. And I'm glad to see so many of my former
6 colleagues on the staff, about what that means for
7 this agency.

8 And so I think that defining privacy is
9 essentially about control of information, which is
10 essentially what Neil did, again, harkens back to a
11 100-year-old definition of privacy and doesn't really
12 fully account for a lot of writing and thinking that
13 has happened about privacy and context and societal
14 values of privacy.

15 But I think our goal as a panel is not to
16 wax philosophical about privacy generally, but let's
17 talk about actionable harm. You know, one of the best
18 kind of written documents about privacy harm was the
19 2012 report and the 2010 staff report of the FTC, and
20 there this agency talked about -- and I didn't work on
21 those wonderful reports -- talked about fear and
22 anxiety and they, indeed, did talk about harm to
23 reputation, chilling effects.

24 And, again, in a 2012 context, that's an
25 important list and it's a list that the FTC still has

1 to put at the center of its work. They talked even
2 about harms to intimacy and dignity, and the FTC has
3 brought cases around that. But I think to talk about
4 this in a 2019 frame, you really, really do have to
5 update the kind of harms that not only the world
6 seems worried about but this agency seems well
7 positioned to address. Manipulation is something we
8 weren't thinking about much in the 2012 context but
9 definitely should gather new light.

10 Four subjects of behavioral testing and AB
11 testing generally, we didn't think a lot about, you
12 know, us being unwitting subjects in psychological
13 testing by giant corporations. And, then, of course,
14 as Neil said, privacy conversations today get to fake
15 news and get to disinformation. And I don't think
16 that's kind of a perversion of what we mean by the
17 word "privacy."

18 I think there's a reason that -- there's a
19 felt need to think about information flows and how
20 they feed things like fake news. I'll pile on, like,
21 three more little things on the pile but refer you to
22 other people who have said much more about it than me:
23 addictive technology, surveillance capitalism, broader
24 questions about the internet of things.

25 Okay. So I will take two minutes to talk

1 about the privacy paradox, though I have about 14
2 minutes' worth of things to say about it, and then
3 I'll invite you to ask me another question and I will
4 continue my answer.

5 (Laughter.)

6 MR. OHM: Let me give you the punch line
7 because I think that will make you want to hear the
8 full speech. I think there's a privacy paradox,
9 which is why economists think the privacy paradox
10 is an interesting question, right, so there's a lot
11 of -- and let me just do this internally, like I'll
12 use the --

13 MR. COOPER: I had an over/under on how long
14 it would take you to insult economists, so...

15 MR. OHM: Yeah, yeah, yeah. No, that's
16 right. And I warned you in email that that's my
17 shtick.

18 MR. COOPER: He was pretty --

19 MR. OHM: I was pretty transparent that
20 that's what I do. And I'll do this within a privacy
21 -- an economist framework, right, in terms of kind of
22 behavioral economics and in terms of the kind of
23 cognitive manipulation that happens around choice and
24 consent. It's crazy to think that any of the
25 preferences that we're measuring in any of these

1 "studies" are revealed. They're manipulated, they're
2 bought, they're controlled.

3 We're talking about companies that have made
4 their great wealth by being the greatest purveyors of
5 information that the globe has ever seen. And so the
6 fact that they can trick people to act against their
7 preferences is not surprising, I think, especially the
8 people who think outside the economic framework. We
9 can continue to dive deep into why economists think
10 that's an interesting question, but I hope we don't
11 spend too much time at this workshop worrying about
12 the privacy paradox because there's all sorts of other
13 indicators that this isn't really meaningful notice
14 and choice that's happening online, and because the
15 FTC has pegged privacy and privacy protection to
16 notice and choice, we should really respond to that.

17 Okay. I've taken too much time. Thank you.

18 MR. COOPER: All right, thank you.

19 Alastair, do you want to jump in?

20 MR. MACTAGGART: Sure, I would. I think one
21 of the problems that, the way I see it, is that we're
22 trying to address the situation where just by living
23 in the world, your entire life is being tracked and
24 manipulated. So when I think about privacy, I think
25 about different stories. So in 2017, the

1 Massachusetts AG settled with Copley Advertising case.
2 They were waiting until women were inside reproductive
3 health centers and then sending them right-to-life
4 chats, saying that's a child, not a choice, right now,
5 don't do it.

6 This feels very invasive to people, and
7 you're trying to live your life. You know, you wear a
8 Fitbit, it knows everything about you, including the
9 state, you think about it, of your relationship with
10 your partner. The in-home device knows everything
11 about what's happening in your home, so it knows where
12 your phone normally sleeps and where your partner's
13 phone normally sleeps, and if suddenly the phones are
14 sleeping in different parts of the house, the
15 algorithm knows before anybody else in your life that
16 your relationship is in trouble.

17 Cars are essentially data-gathering, you
18 know, machines on wheels, and they know how often you
19 eat at a fast food restaurant, how often you go to the
20 gym, and how long you stay there, and what time you
21 get to work and when you leave and whether you've been
22 fired before anybody else knows whether you've been
23 fired. So we have to live our lives. The technology
24 is interwoven into our lives, and we really don't have
25 any choice.

1 And I think the harm we're trying to address
2 is how we do start to get some kind of balance back
3 just by living our lives. And, yes, at some level you
4 could say, well, this is all voluntary, you know, you
5 get to use this technology, you choose to use it, but
6 you're sort of -- your choice that you're left with is
7 to go kind of live in the stone ages and not really be
8 part of the modern world.

9 So I don't think that -- for me, harm is not
10 just physical injury or financial loss, though I think
11 those are important ones, but I think it's important
12 to kind of step beyond that. And so our framework,
13 you know, in terms of this notion that government can
14 only do so much, well, but if you give consumers an
15 easy choice, an easy way to do it, I think you'll find
16 that consumers will flock to it.

17 One of the problems is that it's super
18 complicated to take advantage of your own privacy.
19 I'll give you a little story. I installed Google
20 Photos on my phone to upload photos, and then I
21 thought, you know, I'm going to just log out and just
22 when I have a good connection, I'll log in and I'll
23 upload. I don't want them tracking me all the time.
24 Well, it turns out you can't. Then you go online, and
25 you actually have to -- you have to delete the app

1 from your phone. You can't just have it on your phone
2 and log out and then log back in. You don't get that
3 option.

4 And it's -- these companies make it very
5 difficult for you to take control of your privacy.
6 And so what we think is giving consumers choice that
7 is effective is the way that you're really going to
8 make a change here, and that's why CCPA, the law, not
9 only says make it easy so you have a button on any
10 website that collects your information saying don't
11 sell my information, but it allows for the third-party
12 opt-out.

13 And what that I think is going to create is
14 a world where your browser will easily be able to
15 indicate your opt-out choice, and your device, your
16 phone or computer, will -- well, I mean, computer
17 through your browser, but your phone will also be able
18 to do it, so you won't have to go through the torture
19 of trying to figure out on every website how to take
20 control of your information. And I think that's
21 where, for us, where we're headed, and that's why we
22 went that approach.

23 MR. COOPER: Neil, I know that Paul took on
24 a few things you said, so I want to give you a chance
25 to respond.

1 MR. CHILSON: Sure. So, you know, I think
2 all of these are old ideas, Paul, to be fair. And, in
3 fact, the idea that our technology is manipulating us
4 is as old as technology is. You can follow pessimist
5 archives on Twitter and you'll see just tons of
6 stories, or listen to their podcasts about how TV,
7 advertising, novels, comic books, speech -- writing
8 was a technology that was ruining society by
9 manipulating people in ways that they could not
10 control.

11 And what we've learned over time is that it
12 takes some time to adjust to these things. Law is
13 part of that adjustment; it's not the only adjustment.
14 And, in fact, if it's not done well, it actually
15 retards the progress that can be very valuable.

16 And, so, Alastair, I think you made a great
17 point that we live in this amazing technological
18 environment where a lot of the problems that we've
19 been trying to solve in our lives are now adaptable to
20 being solved through software. And the key to that is
21 information, and in order to get those benefits, we
22 need to maximize the ways that we can share that
23 information, and we also need to respect that
24 information is -- information that involves us is not
25 purely about us.

1 And so my interactions with somebody's
2 computer out there on the internet -- I think
3 sometimes we have this perception that I'm sitting in
4 my living room, I'm browsing the internet, and so the
5 internet's, like, on my computer. That perception is
6 not any more correct than if I wandered out into the
7 streets naked and then said, nobody is allowed to look
8 at me. We don't have rules that say that.

9 We have developed other protections, and
10 we've helped educate ourselves on how information
11 works and what we can do. And some of that means
12 acknowledging that our uses and our interactions with
13 other people, that we need to have a conversation with
14 those people as well and that those choices can be --
15 they can be to choose to not use the service. They
16 can be to choose to do other things. They're not a
17 one-way conversation where if I don't like how the
18 deal is going, I am going to run to somebody else to
19 make that person do things the way I want them to.

20 Sometimes that can make sense when there are
21 certain types of harms, but, again, that's at the core
22 set of harms, not the -- and I don't think we need to
23 perpetuate the idea that we have somehow more control
24 than actually is feasible or possible to achieve while
25 gaining the benefits of that technology at the same

1 time.

2 MR. COOPER: Thanks, Neil.

3 Paul, I want to go back to you. It was
4 something that Neil said, and I think this maybe goes
5 to maybe not the core but this notion of property
6 rights over the data or over the information. Do you
7 look at approaches like the GDPR and the CCPA, and
8 there seems to be at least an implicit entitlement to
9 consumers to have some control over the information
10 that online services collect about them, and that's
11 kind of part of the core.

12 But as Neil posits that, well, do, we
13 necessarily have a right to that information? Is it
14 jointly produced, is it jointly owned? And I guess I
15 would ask more bluntly, are property rights even the
16 right way to think about this?

17 MR. OHM: So property rights are not the
18 right way to think about it. So this isn't about, you
19 know, can we convince people to take \$1.25 and then we
20 can market any way they want. Implicit in the
21 question and I think implicit in the kind of core
22 foundational argument -- and explicit, it was in one
23 of your slides -- is that, when we have something like
24 meaningful and restrained privacy law, we're going to
25 kill the internet as we know it. So let just me riff

1 on that for a second.

2 So I think both the empirical evidence that
3 you had on your slide, but I think, more broadly
4 speaking, is not nearly as strong as is represented.
5 And, in fact, it's always curious to me that the
6 demands for rigor only flow in one direction in this
7 debate, which is we need, you know, more proof that
8 these harms are real harms. They don't feel like real
9 harms, and yet we don't cast the same skeptical eye on
10 claims that if we, you know, have CCPA or if we have
11 GDPR this is the end of society as we know it.

12 When I was at the Federal Trade Commission
13 -- I think I'm allowed to talk about what I said to
14 people because it's what I said to people -- I asked
15 every economist I talked to, usually I would only talk
16 to them once and then they would never come visit me
17 again, I would say what is the empirical proof that
18 behavioral advertising specifically has had a
19 meaningful, appreciable impact on innovation over not
20 having to pay for services, which is usually what
21 people will argue, but over contextual advertising.

22 And I think one of your slides said, well,
23 now we know, it's been proven. It has not been
24 proven. There is a thin read of evidence it's a
25 little thicker than it was back when I was at the FTC.

1 The only people who can do these studies are the
2 people who can get the data from the ad companies.
3 One of the kind of noteworthy studies in 2013 was by a
4 Harvard Business School professor who refused to put
5 it in his scholarship part of his CV; he put it in his
6 paid research part of his CV. And remember, we're
7 talking about contextual advertising which fueled the
8 massive growth of the internet up until about 2007.
9 Sure, there was some behavioral at the time, but
10 companies like Google hadn't yet flipped that
11 particular switch.

12 And so there's a "compared to what" problem
13 whenever we make claims about we're going to kill the
14 internet because it doesn't mean compared to a world
15 with no advertising; it means compared to a world
16 without kind of massive dossiers built about every
17 individual on earth by small companies that have only
18 existed for a year.

19 And so the question is what if -- what if --
20 we could wave a wand and we could say no more kind of
21 third-party tracking just for behavioral advertising
22 purposes? You know what my guess is? We'd have tons
23 of innovation and tons of money, and what's really
24 exciting is the innovators would not be focusing on,
25 you know, to quote a famous Facebook engineer's quote,

1 the best minds of my generation are trying to get
2 people to click on ads. They'd be focused on
3 meaningful content and making a connection with their
4 users and building a community and improving society.

5 And I know that's not the kind of innovation
6 that might excite some people at the end of the day,
7 but it really does excite me. And we have to be
8 really, I think, skeptical of claims and not take it
9 as a given that privacy law kills innovation. I
10 think, quite to the contrary, it can serve innovation.

11 MR. COOPER: I did want to maybe correct
12 the record a little bit. I mean, in fact, I think
13 the research that was shown that I sketched was not
14 that -- kind of the opposite that, actually, that, you
15 know, whether it was Florian Zettelmeyer or Catherine
16 Tucker, Avi Goldfarb that, yes, that behavioral
17 advertising -- an ad with a cookie sells for more in
18 an auction market, generates more revenue, but the
19 lift may not be as large.

20 So the empirical evidence, and certainly
21 there was nothing that I think I said or that was
22 presented or that was presented at the other workshop
23 that suggested that the internet would die if we
24 didn't have behavioral targeting.

25 MR. OHM: Yes.

1 MR. COOPER: So I just want to correct the
2 record as well. Though, I mean, the only evidence
3 that went maybe directly to that was the VC funding
4 study with Liad Wagman and Ginger Jin.

5 But, anyway, with that, I know, Alastair,
6 you wanted to jump in?

7 MR. MACTAGGART: Yeah, I wanted to maybe
8 correct one thing that Neil said. You know, I don't
9 actually think you have any effective choice. You
10 have to use the technology. So this notion that
11 you have some choice about whether to use it is just
12 not -- it's just -- I think it's misleading at best.

13 I think that, you know -- and going back to
14 the contextual versus behavioral, so if you look up
15 Digiday did an article on New York Times -- The New
16 York Times and the behavioral advertising in Europe
17 post-GDPR and showed that its advertising revenue went
18 up in this article, and it came out a couple of months
19 ago.

20 You know, as Paul said, the technology that
21 fueled the creation of Facebook and Google, contextual
22 advertising, no one really finds that very offensive.
23 It's the sense of being tracked and who you are being
24 anticipated before you even know it, that's this kind
25 of weird technology that I think people really are

1 objecting to. And in terms of harms, I couldn't agree
2 with Paul more, everybody always talks about the
3 harms. My question is harms to who. It's not a harms
4 to the consumer. It's the harms to market cap of
5 Facebook and some of these other firms, you know, and
6 I think the last time you ever heard, you know, a
7 consumer saying, you know, my problem with that site
8 is I just don't get enough behavioral targeted ads. I
9 mean, who's ever said that, you know?

10 And so some people really say I never want
11 to see another ad for, you know, the wrong gender
12 product. You know, does anybody really care? I just
13 don't find that is a harm that we should be spending
14 any time focusing on. What we should be spending time
15 -- and the reason -- you know, again, everybody is
16 talking about intervention. Remember, CCPA just gives
17 you choice. If you don't want to do anything, if you
18 love it the way it is, don't do anything.

19 But the reason that all these people -- all
20 the companies are waving their hands panicked about
21 choice is they know that if consumers have effective
22 choice that's easy to implement, they will take it,
23 and that's why everybody is fighting to try to stop
24 that from happening, because they're making so much
25 money selling your information. And people are tired

1 of their information that they're generating just by
2 living their lives being sold and themselves being the
3 market -- being the product.

4 And so that's why I think there's so much
5 sturm and drang about, you know, what will happen if
6 consumers -- don't give them the choice. Well, I
7 believe in consumers and I believe that they will make
8 the right choice.

9 MR. COOPER: Neil, did you want to react?

10 MR. CHILSON: Yeah, you know, I believe in
11 consumers, too, and I believe they are making choices
12 in the marketplace every day right now. But what we
13 do know absolutely from behavioral economists is that
14 choice frameworks matter a lot. And you know this
15 because you made some choices about how you offered
16 choice in doing CCPA.

17 And, so, when you say that it's just about
18 choice, it's not just about choice. It's about the
19 frameworks in which consumers make choices. And when
20 those choices are one size for all the certain
21 problems, and when consumers have widely ranging
22 privacy preferences, different choice frameworks are
23 better for certain consumers than others. And so if
24 we're going to just say here's the one single choice
25 framework that everybody has to do, we're going to be

1 benefitting some consumers, absolutely, without a
2 doubt, and we're going to be harming others.

3 And I just think it's really important to
4 keep that latter group in mind. There are people who
5 don't want to be bothered by certain things, and they
6 want to use these technologies, and they like the ad-
7 driven ecosystem. And like, me, I've often actually
8 said I wish my Instagram feed had a filter where I
9 could just see the ads because I saw this thing I
10 really wanted and now I can't find it. And that is a
11 targeted ad, and I'm a fan. I actually have purchased
12 many things from Instagram ads.

13 So I do think that there are people out
14 there -- and just to get back to the privacy paradox
15 for a second, I agree with Paul. I don't think it is
16 a paradox. I think that the privacy paradox is less
17 about a sort of failure of a consumer to make the
18 proper judgment when they're in real life, and I think
19 it's more of a failure of the researcher to be
20 empathic to people who might make different choices
21 than them in the real life.

22 And so to me, the people who call it a
23 privacy paradox tend to be people who are puzzled by
24 the fact that consumers would say, I like X, and then
25 when they're faced with choices where they have to

1 make tradeoffs, they make a different decision. To
2 me, that's not puzzling. That's how consumers are all
3 the time. It's not a paradox. It's only a paradox if
4 you don't understand why somebody would do that, and
5 that's a failure of the researcher's empathy and not
6 of the consumer.

7 MR. OHM: So because choice is kind of the
8 topic on the table, I mean, my prediction for 2019 --
9 let's do this like a TV show is this is the year where
10 dark patterns really becomes the kind of thing that
11 we're really talking a lot about. And we'll see. I
12 happen to know four or five different teams of
13 researchers who are trying to kind of give a lot of
14 heft and meaning and rigor to what we mean by that.
15 And it really fits within the kind of economist
16 framework.

17 So for those who haven't encountered it as
18 much, right, this is the notion that our choice
19 architectures, our choice opportunities are just
20 completely muddled and clouded by the little tricks
21 that companies play to get you to consent, even though
22 you may not want to. And so this is as simple as
23 putting the yes button in a really prominent dark font
24 and the no in a grayed-out font which is harder to
25 perceive. They're kind of more dramatic examples that

1 Woody Hartzog talks about in his book. Yes, I would
2 like your health service; no, I just want to bleed to
3 death. And so there's all sorts of kind of behavioral
4 cognitive tests.

5 And the most pernicious part of it is how
6 they're completely engineered through AB testing to be
7 far more insidious than any, like, crazy innovator
8 could come up with on their own, and so they're meant
9 to really, really just find you at the most vulnerable
10 moment and get you to click yes because you just want
11 to get to that Instagram ad.

12 And so I've been thinking for my part -- so
13 I've got a little paper coming out with Kathy
14 Stranberg and some of her fellows at the Stigler
15 Center, which is like this economics powerhouse; I'm
16 not sure why I was invited to take part -- about how
17 we might make dark patterns an actionable thing, both
18 through new legislation, but even through the work of
19 the FTC, right, so that if our entire edifice is built
20 on this notion that there is free consent and choice,
21 well, let's take really seriously what happens at the
22 moment when the user consents.

23 And I think what we will lead to -- and I
24 think it will be in a way that even the economists
25 will kind of have to agree with -- that there are some

1 devious tricks that are played at that moment that
2 really do undermine the fundamental notion that this
3 is a contract, this is something meaningful, and this
4 is something that we should premise, for example, FTC
5 lack of enforcement on. And so I think mine will only
6 be one of, like, four or five studies, including some
7 empirical work on this. And I think people on the
8 Hill are probably likely to pay attention as well.

9 MR. COOPER: Well, now that we've solved all
10 of what consumers want and how we should go about it,
11 now I actually do want turn to how we should go about
12 it, kind of switch gears and think about the shape or
13 the form of government intervention.

14 And, Paul, while I have you, you know,
15 there's kind of -- broadly, there are two ways you can
16 regulate ex post enforcement, which in large part is
17 what the FTC does, that we use unfairness and
18 deception to go after practices that are harmful. You
19 know, we use Section 5, but more recently, you have
20 the GDPR, you have the FCC repealed privacy law, the
21 CCPA to perhaps a lesser extent, but a little more on
22 the ex ante regulatory side where they tell firms or
23 marketplace participants, these are things you must
24 do. These are things you have to do.

25 So when we think about either an ex post,

1 maybe harms-based approach or an ex ante regulatory
2 approach, what do you think is the right way to go, or
3 a hybrid of both, or you don't have an opinion?

4 MR. OHM: No, I always have an opinion.

5 MR. COOPER: Okay, that was -- I should not
6 have said that. I forgot who I was talking to.

7 MR. OHM: No, I think it's -- but it's
8 probably an obvious opinion, which is yes and yes and
9 more of both.

10 MR. COOPER: Okay.

11 MR. OHM: But I will -- given probably the
12 only opportunity for me and Alastair to have a little
13 space between us, I'm not as intent on kind of big
14 wholesale FIPPs-space kind of approaches that sweep
15 all companies in. I think they're actually important
16 if they can be achieved, but I think they're neither
17 necessary nor, frankly, sufficient for the kind of
18 privacy that I have in mind, and so I wouldn't
19 personally pour a ton of energy into a nationalized
20 CCPA, probably just because I think the dark patterns
21 problem is going to persist.

22 So something based on notice and consent and
23 choice isn't likely to be meaningful enough, partly
24 because I think the political process will water down
25 anything like that so much. I'm happy with

1 California, and I would like to see it continue to be
2 the law of at least that land.

3 And so let me just say one thing about ex
4 post and ex ante. For ex post, yes, we should
5 continue to be aggressive in our enforcements. We
6 should kind of do more with the dark patterns that I
7 was just talking about. But ex ante, I actually have
8 always said, and I think I depart with a lot of
9 privacy advocates on this, that there should be more
10 laws tailored to sensitive information, so we should
11 have new laws that kind of find the little gaps in
12 types of information that are so deeply sensitive, so
13 connected to provable harm, and yet for some odd
14 reason we don't protect in this country.

15 And so the most obvious one is location
16 information. I mean, there ought to be -- and I don't
17 care which one, any of the right to location privacy
18 acts that have been proposed over the last few
19 congresses, but there should be a kind of fundamental
20 ex ante restriction on what we can do with the
21 specific accurate location information of people.
22 It doesn't mean we would, like, drive out of business
23 any company premised on location information, but it
24 means we would really ramp both the notice and choice
25 that's required, but more importantly the kind of

1 substantive obligations about what to do with location
2 information. It should be like HIPAA; it should be
3 like FERPA. And it's kind of crazy to me that it's
4 not.

5 MR. COOPER: Well, thanks, Paul.

6 Neil, I mean, obviously you began your talk
7 talking about specific consumer harms and that's what
8 intervention should be addressed. So do you have a
9 view on ex post enforcement directed at harm, should
10 there be as Paul suggested? Maybe in some ways that
11 the risk-based regime that the US has in some ways, I
12 mean, you're right, we don't have location, but we
13 have COPPA, which has specific requirements for kids.
14 We have HIPAA, specific requirements for health
15 information. What are your thoughts on harms-based ex
16 post versus ex ante regulatory approach?

17 MR. CHILSON: Sure. So I'll take the
18 opportunity to be in slight agreement with Paul,
19 that's always nice. You know, I do think that ex post
20 has a lot of virtues in the ability to focus on -- to
21 address the challenge of not being able to predict the
22 future, and setting big abstract frameworks into place
23 based on how the technological world works right now
24 is very, very, very difficult. And in 10 years, I
25 think a lot of those frameworks will look out of date

1 at best.

2 And so ex post approaches that focus on what
3 is a particular type of harm that we're worried about
4 or what is a particular type of use that we're worried
5 about, and we're going to watch and see how companies
6 behave, and then if there's injury to consumers, we
7 bring actions. I think that approach has that virtue
8 of not having to predict the future as much. It also
9 has the virtue of not having to be as abstract.

10 So we can look at a specific case, get
11 information about that, and we don't have to have
12 these big-picture arguments about what -- in the
13 abstract, what is privacy harm. We can look at the
14 specific case and say was a specific consumer harmed
15 in this case. And there we have more evidence to work
16 with and it's easier to make a judgment that is just
17 to all parties involved. And so I do think that has a
18 lot to be said for it.

19 And on the dark patterns point, if I can
20 just jump to that, I mean, this is not new to the FTC.
21 The FTC in ad practices does this all the time, right?
22 There are all sorts of dark patterns, and in DMP where
23 -- dark patterns where people get involved in loans or
24 they get involved in advertisement for supplements
25 where there's all these patterns around them. And so

1 I think that's great work. I think there's a lot of
2 evidence that the FTC can draw on around that issue.
3 I think that those parts of the FTC's work have shown
4 that economists bring a lot to the table there and
5 that when you're focusing on --

6 MR. COOPER: Thank you, Neil.

7 MR. CHILSON: -- economists bring a lot to
8 the table there, and you can look and see how to
9 attack certain specific bad practices and bad actors
10 without condemning advertising as a whole or any
11 specific type of advertising.

12 And I will say to Alastair's point really
13 quick, while we're on that, people did find contextual
14 advertising frightening and weird. They did for a
15 long time, and then they didn't. And now in contrast,
16 it's the thing that used to be scary and now we're
17 scared about something else. And so I think that is
18 the trend in privacy and in technology generally, and
19 I expect it will continue regardless of what laws are
20 in place

21 MR. COOPER: Thanks, Neil.

22 And, Alastair, I wanted to move to let you
23 react and also just maybe talk specifically about the
24 CCPA. Obviously, that ended up as an opt-out regime.
25 And I'm curious of what sort of considerations went

1 into -- I mean, it's opt-in for 13 to 16 and then
2 parental opt-in for under 13 because it's in with
3 COPPA, but for anyone over 16, we've got an opt-out
4 regime in the CCPA.

5 So I'll let you react to whatever you've
6 heard but also discuss what went into thinking about
7 opt-in versus opt-out in the CCPA and how you all
8 ended up there.

9 MR. MACTAGGART: Yeah. Well, I think what
10 we wanted to do to the point of -- you know, you don't
11 want to create a law that's stuck in time. So one way
12 to think of CCPA is it really is just a framework that
13 grants the AG in California rulemaking authority to
14 move with the times. And so one of the basic rights
15 are you get the access, right, but really, the one --
16 right around, I think, the most important one is
17 opting out of the sale of your information.

18 And so we were and are pretty agnostic about
19 -- we believe in the consumer, and we believe the
20 consumer can make that relationship with the first
21 party. And so we don't put restrictions on the
22 collection of information by that first party. It's
23 just, you know, the promulgation of that information
24 all the way out into the system where people don't
25 have any control of it and they don't understand or

1 have any control over what's going to happen to that
2 information. And that's where we drew the line, and
3 we said we should give people the right to stop the
4 sale of their information.

5 And, again, going back to the choice, if you
6 don't -- if you like it, if you like getting the ads,
7 there's nothing you have to do, and so there's no
8 intervention. And I think it's a very sort of light
9 regulatory touch in that sense. And, again, we don't
10 stop that first party from collecting the data.

11 And in terms of, you know, enforcement, I
12 think if you look at the sort of ex post enforcement,
13 my point would be just take data breach. It hasn't
14 worked, right? Because -- and you see the security,
15 the data breaches again and again and again. And so
16 what we are suggesting is, look, put a line -- you
17 know, have a reasonable security framework. And ours
18 says if you encrypt the data or if you redact, you
19 know, the names out of the data or if you have
20 reasonable practices and procedures in place, then
21 there's no private right of action.

22 We do have a limited private right of
23 action, right, when calling negligent data breaches,
24 which is just like the cop when he stops you speeding,
25 he doesn't ask you why you're speeding, he just gives

1 you a ticket or she just gives you a ticket. And
2 that's kind of where we are with the data breach. I
3 do think that the whole problem with, like, how were
4 you harmed, Equifax, you know, this data breach, try
5 proving to Equifax that your, you know, identity was
6 stolen six months later because of that data breach.

7 So I think we chose opt-in because it was --
8 I mean, opt-out because we think it's going to be
9 effective. And I was really focused on how do you get
10 something effective, and because we allow for that
11 third-party opt-out, I think consumers are going to be
12 able to do something simple, and that's really
13 important because no one has the time to read privacy
14 policies. No one has the time to go through and find
15 out where to get the settings in this particular app
16 or -- but if you could set it once in your browser and
17 forget it or once in your phone and forget it, I'm
18 convinced that tons of consumers will do that.

19 And that's also why I'm convinced this has
20 suddenly gotten so much attention because companies
21 realize that, wow, this is going to be -- we're
22 profiting immensely from selling everybody's data, and
23 we can't let them have this power to opt out of the
24 sale of that data. And I'm convinced also that these
25 companies are going to do just fine because, again, we

1 don't stop the company from collecting or using the
2 data on their own. So if they can make an argument to
3 you that they need to have your data -- Uber does need
4 to know where I am, Uber does need to track me, Uber
5 does need to have my credit card information, great,
6 that's fine. But do they need to sell it? That's the
7 second question.

8 MR. OHM: Can I say one more thing about ex
9 post because I think it's become fashionable to bash
10 the FTC as ineffective, and call me a Hopeless Homer
11 because I worked here. I think the FTC is really,
12 really effective and smart about the way it uses
13 meager resources. So obviously if anyone in Congress
14 is listening, give them a lot more money so they can
15 really carry out their enforcement mission.

16 I'll also say that I think -- and I'm saying
17 this in a very pointed way -- I think a lot of the
18 community is looking at what happens in the next
19 whenever about Facebook and Cambridge Analytica. I
20 think a lot of minds will be made up on whether -- and
21 probably shouldn't all turn on that one case -- on
22 whether the enforcement mechanism still has life.

23 And then my exhortation to kind of my
24 copanelists is stop challenging and, you know, funding
25 challenges to actions like in the security space. I

1 know this is the privacy conference, not security, but
2 if we want an ex post regime that works, we can't have
3 kind of these pointless, endless litigation about
4 whether or not Section 5 even applies to security.
5 And so that ties the hands of a lot of the enforcers.
6 Ex post can be a lot more than it has been were it not
7 for the challenges like that.

8 MR. CHILSON: I think there are certainly
9 areas in which FTC authority to bring ex post
10 enforcement needs to be shored up given some recent
11 cases. And so I think I agree with you on that. I
12 think I would agree with you on more resources. And I
13 do tend to think that ex post is a better approach,
14 and if we can strengthen that, it solves a lot of the
15 problems better than ex ante, big-picture regulation.

16 And I somewhat disagree with Alastair. I
17 don't think that all of the companies that are worried
18 about the CCPA or the advocates who are worried about
19 it are worried about it because they sell consumers'
20 data and they think they're going to lose money. I
21 think there are lots of reasons to be worried about
22 the implementation costs of CCPA. And I'm not a CCPA
23 expert, and you certainly are, but I've heard many
24 more concerns from many people who don't have a stake
25 in selling consumers' data about the compliance costs

1 that will come about from having to undertake the
2 efforts that CCPA requires.

3 MR. COOPER: Let me -- oh, I'm sorry. And
4 I'm going to let you respond, Alastair, but we're
5 running short on time and I've gotten some really good
6 questions from the audience. And I apologize ahead of
7 time. I probably will not be able to get at all of
8 them, but one was directed at you, Alastair, and I
9 think it fits into the discussion we're having, that
10 if we end up having a lot of opt-out, is that going to
11 lead to a lot of things going behind a pay wall? Or
12 in the sense that -- or the people, they'll be free-
13 riding in the sense that the people who don't opt out
14 foot the bill for everyone else, and then maybe
15 eventually things will -- content will end up behind a
16 pay wall. Do you have any thoughts on that?

17 MR. MACTAGGART: Well, I think it depends on
18 your business model. If your business model is being
19 transparent with consumers and transparent with what's
20 happening to their data, so if consumers don't mind
21 what's happening to their data, I don't think much is
22 going to change.

23 If your business model is based on making a
24 lot of money from selling your consumers' data, well,
25 they don't think that their consumer -- their data is

1 being sold, I think that's going to be -- you're going
2 to have a problem. I mean, I think, look, I think
3 that to go back to this idea of, you know, regulation
4 and the cost of regulation, I think what happens is
5 technology always outpaces society's ability to
6 understand it.

7 And then eventually society sort of wakes up
8 and says in the '50s, wow, a lot of people are dying
9 in car crashes, maybe we should have some auto safety
10 or in, you know, the '70s, they sort of said, gosh, I
11 can't see across LA, maybe we need to have some
12 regulation around, you know, clean air.

13 I think at the time, industry always -- and
14 I'm a businessperson. I mean, I went to business
15 school. I've been a businessperson for 25 years. I
16 think business just tends to react by saying, oh,
17 regulation is going to be super expensive; everybody
18 is going to lose their jobs; this is going to be a
19 disaster. And then, you know what, now you can see
20 across LA, and car makers still make money, and
21 everything has not -- the world has not, you know,
22 ended because we have cleaner air.

23 I think this is sort of a similar scenario
24 where right now there has been no regulation, no
25 really effective regulation around this space in

1 privacy. And I think California is showing up with
2 some effective regulation. And I think, you know,
3 companies are doing what companies always do when
4 there's regulation on the horizon. They say, oh, look
5 at the cost; it's going to be a disaster; people are
6 going to lose their jobs. And the reality is these
7 companies are going to do just fine. They're going to
8 make money.

9 And I think that this is just society waking
10 up and saying, wait, this has gone a little too far.
11 We want to maybe start taking some control back. And
12 that's why we have 630,000 people sign our petition.
13 That's more people than live in Wyoming or Vermont.
14 That's why, you know, it never polled below 80
15 percent. And that's why both houses of the California
16 legislature acted unanimously both times, not a single
17 vote against this, because people understand this is
18 an issue whose time has come. And I think California
19 is just the vanguard, as it has been in so many other
20 areas. And I just happened to capitalize on the sense
21 that people have that this is just out of control.

22 MR. COOPER: So another audience question,
23 and this kind of goes back to something Paul had
24 talked about earlier, and it's really more pointed and
25 specific. Do you think that the dark patterns, the

1 FTC has sufficient authority under Section 5? I know
2 you and Neil had a little back and forth about that.
3 Do you think that there needs to be something
4 additional, or would it fit under current unfair
5 deceptive acts and practices?

6 MR. OHM: Yeah, so I think that dark
7 patterns have extreme enough -- well, obviously,
8 sometimes they're just deceptive. And I take your
9 point, Neil. I did not -- I should have highlighted
10 ad practices and marketing practices having -- they
11 are kind of the experts in DC to think about dark
12 patterns.

13 So first of all, they might be deceptive.
14 If they're really, you know, harmful, they might be
15 unfair. But even if they don't quite rise to that
16 level independently, I think the broader point I was
17 making for the FTC is that they undermine the kind of
18 notion of free choice, and so they might factor, for
19 example, into the cost-benefits balancing that we're
20 forced to do under Section 5(n), right?

21 And so they might be, you know, well, you
22 opted into this and look at all the benefits you got,
23 but you really didn't opt into it because the dark
24 pattern interfered with your ability to make a real
25 choice at that point, right? So, I mean, it's a

1 little round trip through FTC doctrine to make it
2 relevant, but, again, it's couched in the language of
3 economics and so I think has a better chance of kind
4 of having some sort of change within the Commission
5 itself, right?

6 MR. COOPER: Well, in our remaining time --
7 we don't have much left -- I did want to turn to Neil.
8 And, again, we talk about intervention and the
9 potential costs and benefits of intervention. One of
10 the things that comes up, that came up a lot in our
11 hearing in the fall and that you read about both in
12 academic literature and in the popular press is the
13 potential impact on competition of privacy regulation,
14 whether it's -- again, we saw some theoretical models
15 that discuss how it can potentially soften competition
16 if certain -- if entrants have less access to data,
17 less ability to target and poach from incumbents. And
18 then in general, you have the notion that large
19 incumbents may be better able to deal with opt-in --
20 strict privacy regulations than, say, new entrants.

21 So what sort of -- I mean, how should we
22 think about that? Is that an important consideration
23 as we go forward and grapple with some of these ideas?

24 MR. CHILSON: Yeah, absolutely. I mean, I
25 think the effect of regulation on competition isn't

1 just about changing people's business models. Often,
2 it is a way that companies use to cement a business
3 model in place when they are afraid of competition.
4 And so I think Alastair is 100 percent right that the
5 big companies will continue to make money here. I
6 think they will then use that money to use a
7 regulatory framework in the way that they are free and
8 open to do through lobbying to protect their
9 interests.

10 And I think opt-in and opt-out are
11 compliance regimes in which big companies with good
12 brands -- that companies that consumers are familiar
13 with, they can get over that threshold. But new
14 companies that don't have an established brand or less
15 well-known companies or companies who work in a
16 different space but want to move into a new space,
17 they have a much harder time getting into the
18 consumers -- getting consumers to say yes, even if
19 they have a more privacy-protective product because
20 consumers still use the brand signal a lot as a way
21 that they make choices.

22 And so I do think that there's that
23 challenge that regulation can often cement business
24 models into place, that the market pressures, which I
25 think we're seeing there are pressures in this space

1 for companies to act in different ways, that market
2 pressures would push towards naturally, and companies
3 can use regulation to hold back that change.

4 And I'd just add one more thing around
5 CCPA in particular, that many of these rights --
6 one of the challenging things about them is that
7 companies who were collecting some subset of data, in
8 order to avail themselves -- avail consumers of the
9 legal requirements that are in the law may now have
10 to collect more data, and so there is a tension there
11 on how you are improving consumers' privacy by
12 forcing a sort of centralization of information in
13 companies in order for them to be able to validate
14 that it's so-and-so that requested the information
15 about them.

16 And so I think there are some challenges
17 there. I'm not -- I don't want to pick too much on
18 CCPA. I think these are big challenges for any sort
19 of overarching framework that tries to set a single
20 solution for things that the market has and is
21 continuing to find many different solutions for.

22 MR. COOPER: We are basically -- not
23 basically, we are out of time, but I do want to let
24 Alastair and Paul jump in if they want to have one
25 last comment.

1 MR. MACTAGGART: Two things on that. That
2 with all due respect that last comment about having to
3 collect additional information, in multiple places in
4 the act it says that for a single, one-time
5 transaction where you're not collecting personal
6 information, you don't have to collect additional
7 information. This is the kind of thing that people
8 throw up to say, you know, this is going to be a
9 disaster, but if you're collecting personal
10 information, then you've got to be able to re-identify
11 it. But if you're not collecting personal information
12 for a one-time transaction, there's no requirement to
13 keep it.

14 What I'd also say is, hey, before the
15 framework goes into place, 90 percent of new digital
16 ad revenue is going to two companies. They have 79
17 percent of the market right now. So don't talk to
18 me about competition. This law will do the most
19 benefit to increasing competition by allowing some of
20 these companies to start having a little more level
21 playing field by stopping this data moat from just
22 getting bigger and bigger around these giant
23 companies.

24 If Google and Facebook can't ubiquitously
25 track you across every single thing you do on the web,

1 that will have a tremendously pro-competition effect.

2 MR. OHM: I mean, real quick, I think we
3 actually can end with kind of a baseline agreement,
4 although we see it in slightly different ways, which
5 is I absolutely think that we ought to cast much more
6 regulatory scrutiny on giants. So I've written a
7 piece called "Regulating at Scale," which argues that
8 we ought to have laws that do one thing when you have
9 100,000 users, something else when you have a million,
10 and something entirely different when you have 100
11 million or a billion.

12 It's crazy that we have companies with a
13 billion customers, and so they must live up to the
14 highest standards. They may suffer the biggest fines
15 for penalties. They really must be kind of paragons
16 of behavior, partly because of the damage that they
17 can instill on, like, city's populations of people,
18 but partly because of competition, partly, because
19 they have a lot of power, and a lot of our law is
20 kind of geared towards helping them protect that
21 power.

22 And so if the FTC can use its prosecutorial
23 discretion, for example, to go more after giants than
24 after tiny startups. I'm all for that. I think
25 that's a great policy to enact at the Commission.

1 MR. COOPER: Okay. All right. Well, join
2 me in thanking our panelists for the time and great
3 discussion this morning.

4 (Applause.)

5 MR. COOPER: And we will have a break until
6 10:45.

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 THE DATA RISK SPECTRUM: FROM DE-IDENTIFIED DATA
2 TO SENSITIVE INDIVIDUALLY IDENTIFIABLE DATA

3 MS. JILLSON: Welcome back, and thank you
4 for joining our discussion today of The Data Risk
5 Spectrum: From De-identified Data to Sensitive
6 Individually Identifiable Data. My name is Elisa
7 Jillson, and I'm an attorney in the Division of
8 Privacy and Identity Protection. I'll will be
9 comoderating the panel with my colleague, Cora Han,
10 who is also an attorney in the Privacy Division.

11 We are very fortunate to have with us five
12 distinguished panelists: Deven McGraw, General
13 Counsel and Chief Regulatory Officer at Citizen; Jules
14 Polonetsky, CEO at Future of Privacy Forum; Michelle
15 Richardson, Director of the Privacy and Data Project
16 at the Center for Democracy and Technology; Aoife
17 Sexton, Chief Privacy Officer at Tr ata; Shane Wiley,
18 Chief Privacy Officer at Cuebiq.

19 And before we begin the discussion portion
20 of our panel, which will be most of our time together,
21 Jules is going to start us off with a short
22 presentation that covers some of the basics of de-
23 identification, what it involves, what are some of the
24 relevant standards, and what are some of the
25 challenges to de-identifying data.

1 So, Jules, could you please start us off?

2 MR. POLONETSKY: Thanks, and I'll jump right
3 in, of course, with the slide that you expect. Here
4 are all the small sampling of the prominent de-
5 identification attacks that have led many to argue
6 that the identification is impossible in a world of
7 big data. Paul Ohm famously wrote about the databases
8 of ruin that are being created by the failures of de-
9 identification.

10 Reality, of course, is that at some level,
11 we are all probably confident that you can de-
12 identify. There are a million people in the city.
13 Well, that's a pretty big number. We don't think
14 there's a risk. What people mean, we think, when they
15 talk about we're skeptical that de-identification
16 works is they mean that data that actually has useful,
17 valuable, sensitive, practical information in it --
18 useful for research or products or services -- that
19 creates that risk that if not properly minimized, you
20 can re-identify.

21 So let's look a little bit at just a couple
22 of these, and then we'll try to pull out some of the
23 learnings from them that help us frame what is
24 personal and what is de-identified. Let me start with
25 one close to my heart because it led to me becoming

1 the chief privacy officer at AOL many years ago, the
2 researcher who shared online for researchers, a Ph.D.
3 working at the company who shared for researchers a
4 data set where he had eliminated the screen name --
5 the AOL screen name -- associated with months and
6 months of search results. Probably not any data set
7 that a credible de-identification expert would
8 consider anonymous information, but a young, smart,
9 noble, you know, Ph.D. said, well, there's probably no
10 risk in putting this data out.

11 And, obviously, it was trivially easy for a
12 reporter to go through this detailed data set. So I
13 don't know if we learn a lot from it other than if
14 you've got a lot of data, a long amount of data, many,
15 many search results -- people search their own name,
16 addresses, all sorts of information, simply removing
17 the most explicit name, the screen name, the personal
18 name, isn't going to do much to identify. Okay, so
19 maybe not a huge lesson other than dangerous to make
20 public great detailed data sets.

21 More sophisticated and perhaps more
22 interesting for our analysis is Latanya Sweeney's
23 work, Arvind Narayanan and Vitaly Shmatikov work where
24 they conducted what are known as linkage attacks.
25 What is a linkage attack? Well, when you have a de-

1 identified data set and it's joined with a publicly
2 available data set that has information in it using
3 attributes that are common to both those data sets.
4 So what was compelling about the Netflix attack,
5 right, Netflix released for its prize, testing the
6 ability of the public to come up with better
7 algorithms, movie ratings, and dates. Hmm, doesn't
8 seem like a very high-risk set of information, and
9 there wasn't even a lot of it, which was one of the
10 critical sort of pieces. It was simply a number of
11 ratings and dates.

12 And, of course, they should have, if they
13 were doing effective de-identification analysis, said,
14 hmm, is there another data set out there that might
15 actually name some of these people and have more
16 information about them that would enable additional
17 learning that we have placed in this data set. And,
18 of course, the IMDb data set, which has rules against
19 crawling the entire thing, so the researcher didn't
20 crawl the entire thing and say, hey, look how much
21 we've identified.

22 They identified two people because they had
23 a very small sampling. But what they proved was, look
24 at that, these are easier to do than you might have
25 thought. This can be done with a fairly small amount

1 of data and, beware, there are all sorts of data sets
2 out there that you may not be aware that could
3 contribute to a linkage attack like this.

4 Similarly useful to helping illustrate the
5 challenges of de-identification, at least when data
6 sets are made public, was the work of Professor
7 Sweeney where again the linkage attack here relied on
8 the fact that the data sets that were made available
9 included procedures, date of birth, gender, other
10 indirect identifiers that she could use when she went
11 to a very important and essential data set that is
12 publicly available, the voter registration databases,
13 right?

14 Although, they don't have everybody in our
15 population in there, there is, and we all have to take
16 into account anytime we think about de-identification,
17 the fact that there is a data set that has things like
18 gender, date of birth, and your precise address. So
19 it's no surprise that almost every expert who works on
20 de-identification is highly aware that including those
21 sorts of indirect identifiers in a database are high
22 risk because there's this lookup database that can put
23 those sets together.

24 Interesting to note that if one had followed
25 the HIPAA standards, one would not have released a

1 data set that would have included that level of
2 precision. It would have had just, perhaps, birth
3 year and the first three of zip, which might have made
4 that attack much harder.

5 Okay, so let's dig into the basics when
6 somebody looks at assessing a data set and seeks to
7 understand whether it's personal and whether they can
8 de-identify. So, of course, start first with are
9 there direct identifiers. If there's a direct
10 identifier in the database, we understand by
11 definition it's a personal database, so what is a
12 direct identifier? Can I identify somebody in this
13 data set without additional information? Just it's
14 their name.

15 Yes, we might have a John Smith, which
16 doesn't tell us a lot, but is there information that
17 if I look at it without any further research, I can
18 identify this user or can I cross link this
19 information in a trivial way to other information in
20 the public domain? That's a definition from the IS --
21 one if the ISO standards. Experts might add "or
22 widely available," right? So I may not have your
23 name, but if anybody can go ahead and just look up
24 that code online or maybe by paying a small fee,
25 perhaps it's widely available, obviously on its face,

1 we've got an identifier that is personal.

2 Indirect identifiers, for better or worse,
3 are the source of all of these attacks that we've seen
4 on these public data sets. They're also the kinds of
5 data that make data sets precise, useful, valuable for
6 research for products for all the various uses. Sex,
7 date of birth, age. Again, if you're not living in
8 the world of de-identification, why is my sex going to
9 be something that is a high risk? Well, we've just
10 divided the data set right in half -- male, female.
11 Maybe life's more complex nowadays, but obviously all
12 of the indirect identifiers that start letting us
13 slice the data set and enable us to reference external
14 databases for linkage attacks.

15 Professor Sweeney in her work on k-anonymity
16 proposed that for every combination of quasi-
17 identifiers of indirect identifiers that there be at
18 least k records. So this is how we can assess how
19 risky the database is, how many -- if there are a huge
20 number of people with that same set of quasi-
21 identifiers, obviously, there's some safety in that.

22 I'm leaving aside for the moment now some of
23 the de-identification risks such as we saw recently
24 with the census, where although the census was
25 releasing statistical data, the fact that there were

1 so many multiple data sets that could be overlapped
2 enabled experts to narrow some of those cells enough
3 to make smart judgments about individual users. So
4 it's clear that perhaps much of the interesting debate
5 here is less over what are direct identifiers and what
6 happens when I make data sets public where clearly
7 every possible risk needs to be considered, but what
8 happens -- and this is a chart that we did a number of
9 years ago that tried to take a look at how does data
10 actually exist at organizations sometimes.

11 It's explicitly personal. Sometimes it's
12 perhaps got some kind of masked code to it. Sometimes
13 it's got a code that can be looked up. Sometimes an
14 effort has been made to pseudonymize that data,
15 meaning remove those direct identifiers but leave
16 those indirect identifiers. Sometimes that data is
17 protected. Sometimes is's very well protected. That
18 pseudonymous identifier could be a one-time ID. It
19 could be something that's widely used that allows
20 broader linkage. And then we can talk about data sets
21 that go through more statistical protection.

22 So on the next couple of slides, I simply
23 want to show how some of the debate, which ends up
24 being around that outer boundary, do we actually care
25 about covering this data in law? Do we want to

1 protect it at all, ends up missing perhaps some of the
2 more robust debate, which is, yes, we do want to
3 capture it because it's probably not a data set that
4 we're comfortable making public, but once we do put
5 rules and restrictions, what comfort level do we have,
6 whether we call it personal or pseudonymous or
7 something intermediate because frankly it is in many
8 cases a spectrum of risk, what are the rules we want
9 to take?

10 So if we look at just a couple of the well-
11 known pieces of legislation or agreements, Privacy
12 Shield, for instance, recognizing that key-coded data,
13 right, pseudonymized data often used in the pharma or
14 health world, isn't considered under the previous
15 agreement or under the current Privacy Shield a
16 transfer of personal data that is subject to the
17 principles. Okay, interesting.

18 Under GDPR, right, the concept of
19 pseudonymizing data captured as personal, but again
20 subject to more flexible treatment. If I use it in a
21 secondary way, I've got more leeway if I've
22 pseudonymized data, if I'm doing a legitimate interest
23 test, again, if I've pseudonymized it to safeguard.
24 So covered and treated more flexibly.

25 I'll just quickly mention, then, the HIPAA

1 data, limited data set, where, again, recognizing that
2 there are valuable research uses if data is controlled
3 by contracts and not made public, again, although
4 covered by HIPAA, treated much more flexibly,
5 similarly under human subject protection, under the
6 common rule. We've got that flexibility under FERPA.
7 Again, the definition swept wide, but significant
8 carveouts to support the kinds of activity that
9 researchers or others might want to do.

10 I'll go quickly through this just to note
11 that when we think about de-identification, we've got
12 to consider who are the attackers we care about. Do
13 we care that an employee might have additional
14 information? A person in your class who might know
15 something very much about where you sat or how you
16 took the test? Or do we trust that those people are
17 not threats?

18 So who are the attackers? Is it the general
19 public because the data's made public? Is it business
20 partners? Are we worried about actual identity or
21 simply learning more about somebody who is already
22 identified? Can we trust legal and administrative
23 controls? If I come to this from a mathematical and
24 scientific point of view, well, there'll be a data
25 breach, or I don't trust companies or researchers or

1 organizations.

2 If I've proven that this can be done, if
3 someone showed I can hack a voting machine, wow, we
4 care about it, even though there may be other
5 protections around it. Or what place did we put legal
6 or other barriers that might make it unreasonable for
7 the additional data sets to be available? They're not
8 publicly available. They're not widely available.
9 They're protected. They're limited.

10 Very quickly, two of the concepts that are
11 increasingly valuable and interesting, differential
12 privacy, remembering not a technique but rather a
13 weight of measure. Understanding that we can't
14 anticipate every future data set that exists, so
15 measuring the effectiveness of releasing statistical
16 data in a way that doesn't create any more likelihood
17 that there is a privacy impact for you, whether you're
18 in this data set or not. I'll skip going through the
19 details on it because of time.

20 And then, frankly again, another area where
21 researchers are increasingly excited, using
22 homomorphic encryption, a method of being able to
23 combine fully encrypted data sets but yet do your
24 calculations and have valid information. Again,
25 useful for some valuable uses and not for others.

1 So just quick final thoughts. Are we
2 talking about public release, in which case, clearly
3 we come to it with the set of concerns that we can't
4 anticipate every possible method of indirect
5 identifier, we can't anticipate every possible
6 additional data set, and what is our standard? A flag
7 to one of concerns, we certainly have cities today
8 that are eager for smart city regulation, for other
9 scenarios, to capture data sets, for instance, around
10 location. And those data sets, although the city may
11 feel they're confident that they're protected, are
12 subject to Freedom of Information Act requests, might
13 be available for law enforcement, and obviously we've
14 seen risks there.

15 Are we interested in nonpublic controls
16 where maybe a data trust -- like Toronto holds the
17 data where contracts are in place, and do we have a
18 different risk/benefit tradeoff or perhaps precision
19 and accuracy tradeoff? And obviously if I'm doing
20 health research, I'm doing other activities, I may
21 want more precision and maybe comfortable relying that
22 the controls are in place to support the value.

23 So final slide, since so much of the debate,
24 whether we want it or not, ends up being focused on
25 targeted advertising and behavioral advertising. And

1 we'll talk a little bit about it, I think, during the
2 panel, but let's just look at how this framing of is
3 this a direct or an indirect identifier, do we have
4 controls or not that we can trust end up being
5 applied, right?

6 So our first assessment is to look at the
7 kind of unique identifiers that are typically in ad-
8 tracking data -- IP address, cookies, ad IDS and the
9 like. Are any of these direct identifiers, right?
10 Maybe our name is not in there, but are there lookup
11 databases that are so widely available that we can
12 say, oh, by definition this is personal because
13 anybody can go and get this information, or is this a
14 use or is this an identifier that is subject to some
15 restrictions and controls? You can't. There are
16 rules, there are laws.

17 Do you meet perhaps the Breyer test under
18 the European Court of Justice that assessed is it
19 reasonable that this company is going to manage to get
20 this data? Is it blocked by law? Is it blocked by
21 standards?

22 And, then, let's switch to the control side.
23 Are there controls in place -- and maybe for some uses
24 we can talk it -- there may not be -- but other
25 methods of collection with other controls. Maybe

1 there are ways to bound it probably in the bucket of
2 how do we want to treat pseudonymized data.

3 MS. HAN: Great. Thank you, Jules. So you
4 had mentioned GDPR's anonymization requirements.
5 Aoife, can you tell us about Tr ata and its approach
6 to de-identification and GDPR compliance?

7 MS. SEXTON: Good morning, everybody. It's
8 a real pleasure and privilege to be here today and
9 really looking forward to the opportunity to share
10 with you a little bit about Tr ata and its story to
11 date. We're a young company. We've only incorporated
12 -- I've gone backwards, have I? There we go.

13 So Tr ata was incorporated in Dublin,
14 Ireland, just over a year ago. And our investors are
15 Mastercard, IBM, and C3 IoT. And privacy and
16 preserving privacy of the consumer is at the heart of
17 what we do and it's in our DNA, but at the same time,
18 what we're looking to do is to allow innovation to
19 happen and to allow companies to derive data insights
20 and to innovate but not at the expense of privacy.

21 Although a young company, we were recognized
22 last year by our peers and we were awarded the
23 innovation privacy award by the International
24 Association of Privacy Professionals, the IAPP.

25 What was the genesis of Tr ata? Well,

1 anybody who was looking ahead and looking at the GDPR
2 in draft could see that to do analytics under the GDPR
3 was going to prove to be challenging. One of the
4 reasons for that is some of the foundational
5 principles of the GDPR are around purpose limitation,
6 data minimization, and data retention, all of which
7 make it very challenging to collect data for analytic
8 purposes because for analytics you want a large volume
9 of data and you want historical data. And that runs
10 counter to these principles like purpose limitation.

11 Also, typically, when you do analytics, it's
12 a secondary use, so it requires repurposing the data.
13 And under the GDPR, that requires a new lawful basis.
14 And although there are a number of different lawful
15 bases under the GDPR, very often consent is one that
16 is relied upon for analytics, but the GDPR raised the
17 threshold for obtaining consent -- valid consent --
18 under the GDPR because it requires that the consent or
19 you proved that the consent was freely given,
20 informed, specific, and unambiguous. And that can be
21 really challenging to do when you're trying to do data
22 analytics.

23 Also, when you look at trying to do
24 analytics, many companies have decided rather than
25 trying to rely on consent that they would look to

1 anonymize the data for the purposes of conducting
2 analytics. But, again, the GDPR raised the bar and
3 made it more difficult for companies to do
4 anonymization, particularly where they were trying to
5 do anonymization in-house.

6 So the challenge with doing anonymization
7 in-house is that if you have the original data set and
8 then you create a copy or an extract, the regulators,
9 collectively in Europe and also individual regulators,
10 have said that the risk of re-identification will
11 remain because you have the original data set and the
12 extract de-identified data set in one house.

13 So that was the business challenge. And so
14 what was the solution? Well, the solution that was
15 seen and was seen as not available in the market was
16 to allow a third party to independently anonymize the
17 data. And that was really the catalyst which brought
18 about the creation of Tr ata.

19 We talked about some of the safeguards.
20 When Tr ata was being designed, we really started with
21 a blank sheet of paper. How do we create a company
22 that's going to operate independently and is going to
23 be able to anonymize the data but to retain utility?
24 How can we design and architect a company that will
25 ensure that we identify the risks of re-identification

1 and then build in safeguards into the company to
2 ensure that every step along the way we ensure that
3 the risks of re-identification are identified and
4 mitigated and that we can operate independently?

5 So we actually went a step further, and
6 under Irish law, Tr ata is a trust. It's not to be
7 confused with a data vault or a data trust itself. It
8 actually -- its corporate structure is a trust. This
9 means that there is a trust deed that governs how we
10 operate. We have three independent directors on the
11 board whose job is to ensure that we adhere to the
12 trust deed. That deed ensures that no single
13 shareholder can have a majority shareholding to ensure
14 that we operate independently. So that's one of the
15 structures that ensures we can operate independently.

16 In addition to that, it's important to note
17 that we operate as a controller, so we take the
18 responsibility for actually anonymizing the data. And
19 under the GDPR, if we were just a service provider or
20 a vendor, we would be seen as a processor and
21 therefore acting onto the instructions of the
22 controller, and that wouldn't be sufficient to
23 underpin this concept of independent anonymization.

24 In addition, then, we have organizational
25 controls in place. Everything from security by

1 design, privacy by design, and privacy by default have
2 been embedded into the organization in terms of the
3 design and also the operation of the company.

4 And, finally, the technology platform
5 itself, we have state-of-the-art technology
6 platforming -- we rely on IBM -- but also in terms of
7 what the data scientists do to conduct the
8 anonymization techniques, and I'll just talk about
9 that for just a moment. So on this slide you'll see
10 it effectively demonstrates the data journey that the
11 data takes.

12 So in the very first instance, we in Tr ata
13 sit with a customer and we really get to know the data
14 that they hold, the sensitivity of the data, but also
15 the use cases and what it is that the customer wants
16 to do with the data.

17 And once we understand the data, we also
18 understand the direct identifiers and the indirect
19 identifiers. And what we ask the customer to do is to
20 tokenize those and add a salted phrase. The customer
21 then transfers the data securely to Tr ata. And once
22 they've done that, they delete the extract of the data
23 set that they've sent us. We then doubly de-identify
24 the data by also carrying out tokenization and by also
25 a salted phrase. And at that point, we also delete

1 the extract.

2 And this is an important point to mention in
3 the journey because at this stage, we've broken the
4 linkability back to the original data set. The
5 customer still holds the original data set, but now
6 the data that we hold, we've broken the link back to
7 the original data set.

8 So at this point now, the data continues on
9 its data journey. And this is where the data
10 scientists now start the test-driven anonymization,
11 where they start carrying out a battery of tests on
12 the data to try to identify quasi-identifiers.
13 They're looking at motivator intruder tests; they're
14 looking at all the vulnerabilities, what observable
15 features there might be to this data, where might the
16 risks of re-identification lie.

17 At the same time, they're also looking to
18 maintain some data utility. So that's the balance.
19 We have to achieve anonymization, but we are doing so
20 in a way that we retain data utility. Once we're
21 satisfied, the privacy team and the data scientist
22 teams that we've achieved a level of anonymization,
23 the data then carries down through -- into a data
24 store.

25 It's important to note at this point we

1 don't commingle data. The data belongs to the
2 customer, and we are providing analytics back to that
3 customer, so it's not an aggregation. It's not a
4 vault. We don't commingle other customers' data. So
5 at this point, we carry out analytics on the data.
6 And this depends on the use case of what it is the
7 customer needs.

8 Important to note that before anything
9 leaves Tr ata, we carry out further testing. At this
10 stage, it could be differential privacy testing where
11 we add further noise as well to the data. All of the
12 time, we're trying to identify and ensure that there's
13 no singling out linkability or inferences. These are
14 the tests that were set out by the Article 29 working
15 party opinion.

16 The data which leaves Tr ata is only ever
17 going to be in aggregate form, so it's important to
18 note that, or it could be model code. And that's what
19 leaves Tr ata, and the customer then receives that and
20 then can use that for its own business to improve, to
21 innovate its products, its services, perhaps for
22 customer segmentation, for marketing on its own
23 consented database.

24 So we are agnostic in terms of the sectors
25 we work with, the various industries we work with, and

1 the various use cases that a customer might want to
2 use the data for.

3 So final slide. In terms of achieving
4 anonymization, Tr ata has been specifically formed
5 with a view to achieving independent anonymization
6 while also retaining utility for the customer.
7 Achieving true anonymization that preserves privacy is
8 highly complex and difficult to achieve, and it
9 requires real expertise on the side of both the
10 privacy side but also on the data scientist side.

11 Anonymization can assist companies to act
12 responsibly and ethically and particularly to try and
13 rebuild trust with their consumers. So I'll leave it
14 there. Thank you.

15 MS. JILLSON: Great. Thank you very much.

16 So with GDPR, we see one approach to
17 personal data and to anonymization. On the
18 legislative front in the US, it's an open question
19 about how we should be thinking about what is personal
20 data, what is sensitive personal data, and what role
21 de-identification should play.

22 Michelle, I know you have thought a lot
23 about these issues and that in its proposed
24 legislation, CDT has tackled some of these issues head
25 on. Could you tell us a little bit about that

1 approach to legislation and why CDT has taken that
2 approach.

3 MS. RICHARDSON: Sure. Thank you. You can
4 find our draft bill at cdt.org. We started last year
5 and convened academics, nonprofits, and some of our
6 corporate partners to see if we could draft our own
7 federal privacy bill. And we had a few goals. One
8 was to create a single regulation that would apply to
9 everyone, that it would be clear and easily
10 enforceable, but, most importantly, that it would
11 shift the burden from consumers onto the people who
12 are collecting, using, and sharing data.

13 And we borrowed from the FTC when we came up
14 with our definition of covered data, and we do agree
15 that the test should be linkable or reasonably
16 linkable to a person or a device. We did avoid some
17 commonly suggested categorical exceptions, like de-
18 identified information or publicly available
19 information. And we did that for a few reasons.

20 One, we want this to be a really holistic
21 look at data use. If we're going to do this once,
22 probably right and set the parameters, we want this to
23 be broader than we've thought about privacy in the US
24 in the past, what's really more of a consent model.
25 And so that means looking at data use beyond the

1 individual and harms beyond whether a single
2 individual can be tied to data that has some harm in
3 their lives.

4 We want to preserve flexibility for the
5 future. If data processing continues at its current
6 pace, de-identification may become harder and harder
7 to do effectively. And we want de-identification to
8 be encouraged but not necessarily a get-out-of-jail-
9 free card. It is quite a big deal to take yourself
10 completely out of regulation, especially if we are
11 talking as part of legislation that is going to be the
12 sole way to enforce against data practices, both at
13 the state and the federal level. Being beyond that
14 regulation is a serious, serious consequence and
15 should be very rarely, rarely granted.

16 And, besides, there are some issues that
17 were back in the 2012 definition of de-identification
18 that I think are now common and actually will be
19 applied across the board. For example, the way we
20 think about responsibility for third-party access to
21 data and what's a reasonable effort to make sure that
22 the privacy promises you give your consumers carry on
23 to your third parties and service providers.

24 We did, you know, make a list of sensitive
25 information. I know we're going to talk about that

1 later, but we really tried to keep it narrow and talk
2 about a few fundamental rights, things that are
3 outside of the consent model, things that cannot be
4 signed away. And they are, one, access correction and
5 deletion. I know this is something you're talking
6 about tomorrow. Data security, limitation on
7 secondary uses of sensitive information, and
8 rulemaking to deter behavior that could lead to
9 illegal discrimination, including big data processing,
10 profiling, and the use of automated decision-making.

11 And these are the types of issues that
12 crosscut in many ways, even if the information is de-
13 identified. So, for example, if part of your de-
14 identification tactics are not releasing it publicly
15 but keeping it in a sandbox and having tight controls,
16 you would want data security for that information,
17 right, so you could actually enforce your de-
18 identification tactics.

19 And I think we understand that de-
20 identification is going to be a big part of the debate
21 once legislation gets moving this year, and we would
22 encourage Congress to avoid granting get-out-of-jail-
23 free cards, especially for things like pseudonymous
24 data. Processing is becoming more sophisticated, and
25 it's going to be much easier to re-identify this

1 information and make really high-stakes decisions
2 about people.

3 MS. HAN: Great. Thanks, Michelle.

4 So I'd like to switch gears and turn now to
5 a specific type of sensitive data, and that's health
6 data. Deven, can you tell us about Citizen and its
7 approach to health data and de-identification? And
8 also given your long history with health information
9 from working at HHS, is there anything else about
10 HIPAA that you think should inform our discussion?

11 MS. MCGRAW: Sure. Thank you, Cora.
12 Citizen is a new company. We are only about a year
13 and a half old and not yet available to the public,
14 although, we do have about 50 beta users of the
15 platform. We're building a platform that enables
16 individuals to be able to gather all their health
17 information from all the places where they've been
18 seen and to have that data then be under their control
19 and able to be used by them and then also shared by
20 them.

21 We're starting with cancer patients for lots
22 of reasons. One big reason is because those are among
23 the most motivated patients to actually have their
24 data and need it to seek second, third, fourth, and
25 fifth opinions to be able to determine eligibility for

1 clinical trials and then ultimately to be able to have
2 that data used for research purposes so that what
3 they're going through is not -- you know, that they
4 can essentially donate their data so that the people
5 coming behind them have a better chance.

6 In terms of what we will do about de-
7 identification, it's actually -- you know, we're
8 fortunate to be a young company when all these
9 discussions are taking place because we can learn a
10 lot from what has been done in the past, but because
11 we're really designing a platform where we will have
12 relationships with individuals and want to gather
13 their trust. I think for a lot of people they sort of
14 no longer trust that there's a line between
15 identifiable data and de-identified data, and they
16 want to have some control even over de-identified data
17 as well.

18 So whatever techniques that we will use to
19 de-identify data -- which we will because we want to
20 provide our users with options about sharing de-
21 identified data, and we want to be able to when we
22 present that option to them to tell them your data has
23 been de-identified in accordance with some ideal
24 standard that is out there and measurable but also
25 letting them know that de-identification does not

1 reduce risk to zero, that there still is some risk
2 that that data could be re-identified, and are they
3 still comfortable making their data available for that
4 purpose.

5 So in many respects, treating it a lot like
6 the law requires identifiable data to be treated, but
7 yet on the identifiable data level, we want to give
8 people a lot more granularity with respect to their
9 uses and disclosures of data in that regard, whether
10 that's through categories of uses, differentiating
11 between services that might be something they want to
12 take advantage of as individuals versus services where
13 there's data and they want to be able to allow their
14 data to be used for certain purposes along with other
15 cancer patients' data on the platform.

16 So lots of things to think about, but
17 we're going to be treating de-identified data as
18 though it does raise some residual risk and -- because
19 it does -- and giving people some choices with respect
20 to how they share that. I get asked a lot what's the
21 business model if you're not, in fact, going to de-
22 identify the data and sell it as a way to support the
23 platform. And ultimately we want to empower our users
24 to be able to monetize their data if they want to.

25 And we will take some cut from that,

1 essentially, a broker's fee of putting patients who
2 have valuable data together with people who want that
3 data. And that data doesn't have to be de-identified
4 necessarily in order to create that monetization
5 opportunity. In fact, a lot of times for a cancer
6 patient, what is valuable is the identifiable data,
7 but obviously it's a challenge to make that clear to
8 folks because these issues can be quite complicated,
9 but that is our plan for moving forward, is to give
10 people choices, even with respect to de-identified
11 data, and then also to be very transparent with them
12 about what it means for data to be de-identified in
13 terms of their risk.

14 I thought Jules did a great job around
15 talking about HIPAA and particularly emphasizing that
16 the re-identification techniques that Latanya Sweeney
17 used of Governor Weld's data were done before HIPAA's
18 standard on the safe harbor was established. But
19 having said that, you know, HIPAA has in some respects
20 stood the test of time with respect to, you know,
21 health data that is generated in the traditional
22 healthcare system, traditional actors in healthcare in
23 the United States, doctors, hospitals, health plans,
24 pharmacies, not pharmaceutical companies because
25 they're not covered.

1 Nevertheless, it's a standard that was
2 created in 2000. And even at the time that it was
3 created, the agency -- the Department of Health and
4 Human Services -- got a lot of questions about whether
5 they should decline to regulate data that were de-
6 identified. And it's kind of amazing actually some of
7 the preamble language around the promulgation of that
8 very first privacy rule where they came up with the
9 two methodologies for de-identifying data. And,
10 again, the Department was specifically asked, there is
11 no zero risk. And they absolutely acknowledged it,
12 even at the time.

13 This was in early 2000s, way before we had
14 the amount of data that we have out in the world today
15 that can be used to re-identify. The Department was
16 challenged in that regard, and they deliberately made
17 a policy choice that HIPAA envisions a reasonable
18 balance between the risk of identification and the
19 usefulness of the information. So they consequently
20 created two ways to -- created a legal standard around
21 de-identification, which is either not identifiable or
22 no reasonable basis to believe that data can be
23 identified to a particular person.

24 And, then, again, two methodologies. Safe
25 harbor, take out 18 specific identifiers and have no

1 actual knowledge that the data set can be re-
2 identified and you are home free. The regulations
3 disappear. And because HIPAA then doesn't regulate
4 that data, it will be subject to potentially
5 additional regulation by the Federal Trade Commission,
6 for example, if their jurisdiction applies in that
7 particular context. But, again, the data has at least
8 been de-identified in accordance with one standard.

9 And then the other methodology is expert or
10 statistical methodology, where the application of
11 statistical methods reduces the risk to very small.
12 Never was zero. Never, ever was zero. Once you have
13 reached that reduced risk of very small, essentially,
14 again, your data are de-identified, and they fall out
15 of the protections of HIPAA altogether.

16 Jules mentioned in his presentation a type
17 of data set called limited data set under HIPAA, which
18 I used to call it the close cousin to de-identified
19 data because it has a safe harbor-like approach.
20 Sixteen categories of identifiers need to be removed
21 as opposed to 18. There are just two that are allowed
22 to remain in a data set, and then a required data use
23 agreement that commits the recipient not to re-
24 identify the data.

25 So some would argue that that actually

1 creates a stronger set of protections around data for
2 which the risk has been reduced significantly, but
3 with that contract, you at least have a contractual
4 obligation not to re-identify the data, whereas with
5 de-identified data, it falls out of protection all
6 together and there are no penalties associated with
7 re-identifying that data.

8 But what I have found in many, many years of
9 working with HIPAA entities is that they like the
10 certainty of the de-identified -- of following the de-
11 identified data because it comes with that get-out-of-
12 jail free card of no regulation at all, whereas the
13 limited data set, it is only available for certain
14 types of purposes -- research, public health, and a
15 category of uses called healthcare operations.

16 And you also have to enter into a contract
17 with the recipient, which, you know, again, if you've
18 worked inside a company entering into a agreement
19 where you can get everyone agreed, can take months to
20 do. And so de-identified data, if you are able to use
21 it, easily is something that again it's just this very
22 easy methodology.

23 I'll make one more point and then I'll stop,
24 and that is safe harbor has been the method of de-
25 identification that has probably gotten the most

1 amount of criticism with respect to the HIPAA standard
2 because it sort of treats -- again, it was created
3 back in 2000, identifies 18 categories of identifiers,
4 a few of which are broadly stated, but nevertheless
5 the assumption that you can create a standard in 2000
6 and think that it is still as viable in 2019 as it was
7 at the time just feels a bit -- is naive the word to
8 use? I'm not sure that that has necessarily stood the
9 test of time.

10 But even when the HHS created the safe
11 harbor standard, they expressly acknowledged that they
12 were doing something that would be easy for less-
13 resourced entities to use. And because de-
14 identification is a pathway to zero regulation, a lot
15 less constraint on data. You create this enormous
16 incentive coupled with a very easy methodology for
17 significantly reducing data risk.

18 And that, to them, was a sort of magic
19 combination for encouraging again less-risk data to be
20 used for a broad set of purposes, which in healthcare
21 is often really critical. I mean, that's one thing
22 that is somewhat different about healthcare data is
23 that it has both the potential for serious misuse in
24 terms of it getting out and people knowing private
25 things about individuals, but on the other hand there

1 is a lot of value to being able to use it for multiple
2 purposes around public health research as well as
3 business analytics.

4 MS. JILLSON: Thanks, Deven. When we think
5 about health information, we often think of that as
6 the archetype of sensitive personal data, but let's
7 think more broadly about what makes information
8 sensitive.

9 And, Shane, I'd like to direct this one to
10 you initially. During the first panel, one of the
11 panelists mentioned that perhaps a privacy regime
12 should focus on what data is sensitive and have more
13 protections geared toward those specific types of
14 data. And that panelist mentioned, in particular,
15 location.

16 And, Shane, could you tell us a little bit
17 about Cuebiq, its approach to location information in
18 particular, and data analytics? And then let's expand
19 that even a little bit more and talk about what makes
20 data sensitive. Is it consumers' expectations around
21 that data? Is it the actual or likely uses for that
22 data? What makes it sensitive?

23 MR. WILEY: Well, great. So, one, thank you
24 to the FTC for inviting us here today. Thank you to
25 Paul Ohm for setting me up as the guy representing a

1 location intelligence company. So Cuebiq provides
2 marketers location-based, artificially intelligence-
3 driven analytics and measurement to map and measure
4 the customer/consumer journey, helping marketers
5 answer strategic questions and make the right
6 decisions in order to help influence consumers through
7 the sales funnel.

8 More specifically, Cuebiq's Clara platform
9 is fueled by data collected via an SDK or software
10 development kit that's integrated with our roughly 200
11 app publisher partners. We require users' consent to
12 our collection of their location information and honor
13 many pathways for a user to revoke that consent in the
14 future if they so choose. So from a sensitivity and
15 de-identification point of view, precise location data
16 provides unique challenges when compared to other
17 types of data that may be collected.

18 So like we've talked about already a bit on
19 the panel while other forms of data collection often
20 focus on de-identification, primary identifiers or
21 direct identifiers, and at Cuebiq, we focus on that as
22 well.

23 The risk within precise location data is the
24 data itself can in some cases be used to link to
25 publicly available records to reverse engineer

1 identity. Not going to go into it deeply, but
2 reference a 2013 MIT, you know, study that looked at
3 this problem and demonstrated that with as few as four
4 location data points, they could reverse engineer
5 identity to about 95 percent of the data pool that
6 they were investigating.

7 So when looking at this, you're going to
8 hear me speak to several concepts. So, first,
9 concepts like nonderivative identity systems. Aoife
10 touched on this a bit when talking about tokenization
11 and salting, so I'll talk about that a bit as well,
12 especially in the world of mobile, where we have a
13 mobile ad ID.

14 I'll also talk about differential privacy
15 concepts outside of the aggregate-only outcomes.
16 Right, so that's mostly how we talk about differential
17 privacy, but at the root of differential privacy or
18 Laplace, the equation is randomization and how can we
19 apply that to location data to help de-identify it.

20 And then on sensitivity, this is the more
21 difficult discussion point because there's so many
22 different points to touch on, but location sensitivity
23 poses interesting challenges when compared to content
24 or interest-based category sensitivity. Not to say
25 that those are black and white areas either, but

1 location sensitivities, you know, have additional
2 dimensions of complexity.

3 So let's first talk about nonderivative
4 identity systems. And this is what I would recommend
5 to all companies collecting information, especially
6 from mobile devices. If you're collecting something
7 like the mobile ad ID, I'm using that generically on
8 IOS, that would be the IDFA or ID for advertiser, and
9 on Android, that'd be the GPASA ID or the Google Play
10 Store ad ID. But I'll just use mobile ad ideas as a
11 sort of unifying term.

12 If you're collecting that information, it's
13 highly recommended that you immediately use a
14 nonderivative identifier internally. So this is
15 basically creating a mapping table. As a starting
16 point, this is a concept similar to tokenization where
17 I'm creating an identifier that I'm going to use
18 within my organization that it's only tied to the
19 mobile ad ID as a single mapping table. From that
20 point forward, the data journey within my organization
21 should use that internal ID.

22 So at Cuebiq, we call that the Cuebiq ID.
23 But there's nothing within that ID that would allow me
24 to reverse engineer it back to the mobile ad ID. It's
25 not a direct hash or a direct salted hash of the

1 original identifier. It's purely map table-driven.
2 That way, if I delete that entry in the map table, at
3 least the identifier, there's no pathway back to that
4 original mobile ad ID.

5 We implemented similar systems at Yahoo.
6 I've heard many other organizations begin to move to
7 these nonderivative identification systems as a way of
8 creating an insulation layer between sort of the real
9 world production identifier and an internal use
10 identifier, to help get outside of those GDPR
11 complaints, that if you have the raw data that you
12 can't, you know, be 100 percent confident that you
13 have anonymized information.

14 Now let's get into location information
15 itself. I'm going to put it into three categories,
16 this is sort of how we think about it at Cuebiq, but I
17 think you could use these and express them in other
18 applications as well. The three buckets are going to
19 be in sort of a state-of-art concept or acronym in
20 location data is POI, or points of interests. So if
21 you hear me use that acronym, just add that to your
22 acronym soup for today. But POIs fall into sort of
23 three categories for us. We have known nonsensitive,
24 known sensitive, and then unknown. So a known
25 nonsensitive would be something like Macy's,

1 Starbucks, McDonald's. This is a retail location that
2 we know a device has visited. We don't deem it to be
3 sensitive.

4 In the sensitive category, so known
5 sensitive, we really sort of have two areas. We have
6 home and work, and we're going to spend special time
7 talking about that with respect to de-identification
8 because that tends to be the weak link of location
9 data is the home location. But there are other sort
10 of known sensitive locations -- adult content-oriented
11 establishments, disease-specific medical facilities,
12 places that are predominantly populated by children.
13 These would be all areas that you would put onto a
14 known sensitive list and you might blacklist those,
15 such though as you see information come in from those
16 locations, you expunge it immediately.

17 With home and work location, a de-
18 identification technique we use -- and, again, this is
19 borrowed from differential -- privacy is consistent
20 randomization. So in the US, the US Census created a
21 great construct for us to use. If you break the
22 hierarchy down for how information is tracked within
23 the US Census, it starts with a track, then it goes to
24 a census block group, and then you get to the census
25 block itself.

1 Now, if you're trying to find a way to sort
2 of group them, a census block is most analogous to a
3 postal code, a full nine-digit postal, five-plus-four-
4 digit code, which generally is city block/side of
5 street. So that's how specific generally zip-fours
6 are. There are places that break that like New York
7 where you can have very large multistory buildings
8 that have multiple, you know, zip-fours of their own.
9 But generally in the United States, that's how we
10 break it down.

11 But within that, Cuebiq works to up-level
12 any home or work information within a census block
13 group, which generally gives us somewhere between 600
14 and 3,000 individuals within that group. Right? To
15 give us some degree of insulation, that our analysis
16 can still work, marketers can still understand general
17 patterns of movement, but they don't need to know
18 specifically where someone lives. And by ourselves
19 expunging the original information, only working with
20 the up-leveled information, that protects us as well.

21 As we move to the last category of unknown,
22 this is where we use consistent randomization in a
23 different way, but this is -- again, we don't know
24 where this location resolves to, right? It could be
25 in the middle of a field, the middle of a freeway.

1 It could be a point of interest that we've just not
2 yet categorized. So before any of that information
3 would be shared, like through our "data for good"
4 program, where we work with government and academic
5 institutions to help, you know, with programs like
6 city betterment or disaster relief efforts, we do find
7 a point. We take the actual lat/long and randomize it
8 both on vector and on distance within that area. And,
9 again, here, census block group can work.

10 More interestingly, on the scientific side,
11 we'll use something called a geohash. If you've never
12 heard of that, it's more of a grid-based way of
13 looking at our globe, where there are different
14 rectangles and the level of the geohash dictates the
15 size. Our general randomization is on geohash level
16 6, which is about a 1.2 kilometer by .6 kilometer
17 rectangle. But that way we can take these unknown
18 locations, move them into a random point within that
19 geohash 6 rectangle, preserve some degree of path
20 analysis, but again never know that someone dwelled or
21 visited any specific point within that geohash 6, so
22 sort of protecting the unknown sort of category. So
23 that's sort of a general way of looking at de-
24 identification. I'm sure we'll go deeper on that
25 today.

1 On sensitivity, this is one that we struggle
2 with, I would say, the most. Struggle in that there
3 are no bright lines. I think it's very clear and easy
4 for reasonable minds to agree on the black and the
5 white side spectrums of sensitivity. Even when I was
6 at Yahoo and we had our sensitive categories council,
7 this was always one that was interesting from a debate
8 perspective and from a cultural perspective on who
9 would find what category sensitive versus not.

10 Obviously legal-protected areas, those are
11 easy. I'll share one that's more complex, more
12 present. CBD oil dispensaries. So something that's
13 even at the federal level has been recognized as
14 acceptable, so we don't have sort of the state versus
15 federal problem that we would have with, let's say, a
16 marijuana dispensary. Do we want to allow any sort of
17 retail tracking in that area?

18 We ultimately decided no, new area too
19 sensitive for us at this time. We want to wait to see
20 where cultural acceptance, you know, drives in this
21 area, but it just gives you a general sense of context
22 and I would say cultural norms as well as sort of time
23 sensitivity to that cultural norm. You know, much
24 like the first panel discussed, things that are new
25 are the things that are most disruptive, I would say,

1 from a sensitivity perspective. Things that are new
2 tend to have the higher sensitivity.

3 Brighter lines are easier areas for you, are
4 some of the ones I talked about earlier in the known
5 sensitive category. Anything around children we
6 generally stay far away from. We do have mixed
7 audience locations, and this is one that we debate, so
8 something like a mall or a movie theater. Would that
9 be something that should be something that we would
10 have white-listed in our POI database?

11 So we'll go -- I'm sure there will much more
12 lively discussion around sensitivity, but I think
13 there are multiple dimensions into it, and location
14 adds a new complexity because where you go or where
15 you dwell in sort of location world nomenclature may
16 say a lot about you. I don't know -- the fact that I
17 know you go to a theater doesn't mean I know which
18 theater you went to, or, I mean, which movie. But,
19 you know, there could be other inferences drawn from
20 other places that you visit.

21 But we at Cuebiq primarily focus on the
22 retail space, so we feel that's generally deemed
23 nonsensitive. So from that point, I'll leave it
24 there.

25 MS. HAN: Thank you.

1 So I would like to push a little deeper on
2 the topic of sensitivity and direct this next question
3 initially to Michelle, but then I'd like to get the
4 thoughts from the rest of the panelists as well.

5 Some stakeholders have proposed that privacy
6 regulation be scaled to data sensitivity. What do you
7 think of that approach and do you think it requires a
8 clear definition of sensitive data, even given what
9 Shane has talked about with the lack of bright lines?

10 MS. RICHARDSON: Yes, so we are proposing
11 that there be heightened protections for sensitive
12 data, but I want to say up front that doesn't mean
13 that there are no protections for less sensitive data.
14 I think people who are concerned about creating the
15 list, right, means anything that's not on the list
16 isn't protected, so you could ensure individual
17 control, data security, fair data use over all
18 personal information.

19 And then the debate becomes there's
20 something so sensitive that we lift it up out of even
21 those protections for heightened controls. So for us,
22 we look at things like is the information immutable,
23 is it intimate, is it the type of information that
24 high-stakes decisions are made on? It can be just a
25 data set or it could be data uses. And that is

1 something that could go onto a clear list.

2 So clear lists are helpful. Right? And I
3 find people usually conflate what should be on the
4 list with how they want to use it, and they can't
5 disentangle it. So it's better to say, no, let's just
6 define what the sensitive data is and the consequences
7 for dealing with it later, right? And for us, the
8 information that we found most sensitive data were
9 precise geolocation.

10 This is such a proxy for almost everything
11 you do in your life -- you know, your doctor, your
12 romantic partner, your job, your political
13 affiliations, what church you go to, but biometrics,
14 children's information, health information, and not
15 HIPAA health information but a broader definition of
16 information that reflects your well-being or
17 information used to make decisions about your health
18 treatment, right? The content of communications or
19 the content of audio and visual.

20 And this is the type of information that we
21 would recommend you put purpose limitations on, right?
22 So if you get to the second part of the question of,
23 well, then, what's the consequence for being
24 sensitive, we think this is the type of thing that
25 could be clear and actionable for actors, all sorts of

1 sizes, and gets us outside of the consent loop that we
2 keep being stuck in otherwise when we talk about
3 privacy laws so frequently here in the US.

4 MR. POLONETSKY: So I'll jump in, and I
5 guess I'd add that, look, there are clearly some what
6 the Europeans labeled special categories of data that
7 we've got some consensus are likely to often be risky.
8 I think where the Europeans probably left out some
9 nuances, there are actually still some beneficial,
10 we'd all agree, are probably valuable uses of that
11 that maybe are not feasibly subject to consent but
12 where we might in a transparent way say if you went
13 through an ethics review, if this was used for a
14 certain sort of research, if it was pseudonymized
15 where we'd want to see and have that safety valve as
16 opposed to, sorry, go get a law passed because this
17 particular use we didn't think of it at the time.

18 I'd say beyond that, right, everything is
19 arguably sensitive and is arguably nonsensitive. We
20 heard McDonald's. I keep kosher. If I was at
21 McDonald's, which is the classic nonkosher place to
22 get a, you know, hamburger and cheese, I would be
23 embarrassed, right, or could be shamed in my world of
24 kosher eaters, right?

25 And so the reality is, drawing the line

1 between all the other categories that may or may not
2 be sensitive or might be sensitive for particular use
3 and not for another context or with the particular
4 user ends up, I think, being enormously challenging.
5 The legitimate interest notion that is actually the
6 center of GDPR in most uses, even though we talk about
7 consent an awful lot but is the basis of the sort of
8 the engine of GDPR, forces that sort of assessment
9 depending who you are and who the user is and what the
10 risks are, and you've got to document that.

11 One nice thing about perhaps the drafters of
12 the Washington State legislation is that it sort of
13 forces that sort of assessment. The FTC authority in
14 some way when companies have to assess, you know,
15 fairness to some degree, it's not a foreign notion to
16 us that you've got to do that benefit/risk assessment
17 less that particular use be fair.

18 So I'd argue there's a set of special
19 categories that we all agree and that's more likely to
20 be a narrow set that demands, you know, a higher
21 standard with an appropriate hard-to-get safety valve
22 for the sorts of uses that are truly defensible and
23 that the rest of this bucket, because everything can
24 end up being in there, one location, it could be an
25 abortion clinic, the ad targeting example that was

1 mentioned earlier, clearly, you know, highly
2 unhealthy, but can somebody be targeting all
3 facilities where someone might want a ride share ride
4 home, right, or where someone might be selling, you
5 know, some particular, you know, air conditioning
6 device and you've got different categories because
7 there are some reasons to logic, though?

8 So you can -- almost any piece of
9 information -- my retail shopping on my loyalty card
10 is probably truly revealing of my health, you know, in
11 a real serious way. On the other hand, there are
12 clearly friendly uses. So I'd argue if we go broad on
13 sensitive, we end up having to anticipate and carve
14 out a whole range of uses. We're better off setting
15 an accountable process that forces that sort of hard
16 balancing and it recognizes safeguards and the
17 differences in context.

18 MS. RICHARDSON: Well, actually, let me push
19 back. I think this is the concern, right? If it's
20 just a process, I'm afraid it's going to sound exactly
21 like what we just heard, that it's different for every
22 individual so actually we can't create any
23 presumptions on certain data sets at all. If we can't
24 get to that point during this process, I'm not sure
25 the value of passing a federal privacy law and that

1 there have to be some baseline protections for certain
2 types of data. Otherwise, it will not be worth the
3 trade that we're asking for here, right, to intervene
4 and repeal probably 50 different state laws on data
5 security and privacy.

6 The goal should be to maximize the
7 relationship that a consumer has with the company that
8 they are using a service for and that primary
9 relationship. And people are very understanding.
10 They understand their Fitbit has their health
11 information, right, or Google Maps has their location
12 data. It's the secondary uses that are riskier that
13 upset people and that you could clamp down on while
14 still allowing companies to innovate, offer the
15 products people want, and have an iterative process to
16 make them even better.

17 MR. WILEY: Yeah, just to speak to the
18 sensitivity spectrum a bit, so at the NAI, we spent --
19 this is circa eight years ago -- we spent a good solid
20 three years trying to develop a sensitive categories
21 list. And it ended up being so subjective and, again,
22 even in the broadest swath's language, how language
23 use may describe or not describe something, blood
24 management versus diabetes, there were so many
25 difficulties in that process that we went a different

1 route. And we decided that anything that was
2 suspected to be sensitive required transparency. Let
3 the world judge. Let your users judge.

4 This is where, you know, if you were
5 participating in any categories that may be deemed,
6 you know, sensitive, you had to post those, you know,
7 publicly and say these are the things that we target
8 ads against and then allow that sort of sunlight as
9 the best disinfectant, you know, play out.

10 MR. POLONETSKY: But to agree with Michelle,
11 there are special categories, either in NAI or in GDPR
12 or in sort of my comments. Clearly, there are those
13 that ought to be taken off the table, and I don't
14 think anybody disputes that. The only question is,
15 what about everything -- everything -- else because
16 I'd argue there's nothing that is never sensitive in
17 some way in some form.

18 And the question is, you know, do we have
19 grade two medium and grade three medium, or is that
20 just a door that becomes too complicated and are you
21 better off setting an accountable balancing test for
22 the data that is not always, by definition, sensitive.

23 MS. JILLSON: So in the interest of time,
24 let's move from sensitivity to de-identification. And
25 could you advance the slide, please? So in 2012, in

1 the FTC's Privacy Report, the FTC laid out this
2 framework. The data falls are -- data falls outside
3 the scope of the framework, that is, it's not
4 reasonably linked to a specific consumer, computer, or
5 device if these three conditions are met.

6 Do you think that this is the right
7 approach, and do you think that this approach is still
8 workable today, and have problems arisen with trying
9 to adopt this approach?

10 MR. POLONETSKY: I want to strike out the
11 word device unless it's a device that is actually
12 linked to a user because there's lots of devices all
13 over the world that are not personal because they're
14 public wi-fi or an IOT device that doesn't actually
15 get attributed to an individual, but otherwise I think
16 it's pretty good.

17 MS. MCGRAW: I have some questions around
18 the company requires -- I remember this in 2012, and
19 I'm sure I applauded it at the time. And now that I'm
20 inside a company, I have questions about number three.
21 The company requires any downstream users of the data
22 to keep it in de-identified form. That puts a lot of
23 pressure on companies to chase down all the places
24 where it potentially would be accountable for what a
25 downstream user does with the data, whereas if this

1 were a sort of more universally applicable standard
2 that applied to recipients and said if you have it --
3 if you received it in de-identified form and that is
4 the basis upon which you process this data, then you
5 have to keep it in that form and can't reidentify it
6 as opposed to always putting the onus on the
7 discloser.

8 MR. WILEY: In practicality, this list is
9 always broken down into three pieces: technology,
10 pieces, and contracts. Outside of the public
11 disclosure, and that's why I think point two is
12 important, but I think that's where we have to go a
13 little bit further. I'd say this is good as a high
14 line rule. I think we can go a little bit further to
15 state that, you know, reasonably here needs some help.
16 What is reasonable or not reasonable, I think, needs
17 more clarification, needs more guidance to industry.

18 And then lastly, it requires any downstream
19 users of the data. Again, I think this is the
20 contractual side of it, but I would go a little bit
21 further than that as well. You could, again, cross
22 sensitivity into this and require more than just a
23 contract. You could require third-party audits,
24 participation, organizations that require, you know,
25 annual audits, those type of safeguards beyond just

1 the contract.

2 MS. RICHARDSON: And I think the commentary
3 in your 2012 was good. The NISTIR report from a few
4 years ago on de-identification added more detail,
5 right? And I think we're headed in the right
6 direction of identifying what's reasonably
7 identifiable. And it should scope two things like the
8 type of information, how it's going to be used, the
9 sophistication of the data handler.

10 And I think we could be much more aggressive
11 about this. De-identification is not something that
12 is going to be used by very small players, right? It
13 will be easier to just say here is your access
14 correction and deletion rights and a few other things
15 that it is to go through de-identification, right? So
16 these are advanced data processors who have
17 professional services who can make this happen.

18 So I think we should be expecting much more
19 of them. As far as sort of the downstream uses, I
20 think we need to say not just contractual obligations
21 for the third parties that you give in a private
22 space, but if you are going to make the information
23 public, for example, right, or maybe throw it up in
24 your API where literally millions of developers are
25 interacting with it, you are then taking on a burden

1 and a forward responsibility to make sure that
2 information stays de-identified.

3 And you should be responsible, for example,
4 on a regular basis to be running that data against
5 publicly available information or data sets and other
6 things to make sure that it stays de-identified. You
7 can no longer throw the data out there and say you're
8 no longer responsible for it. I think that was
9 something that was said quite frequently just a couple
10 years ago. But looking at things like Cambridge
11 Analytica, it has changed people's expectations of
12 what original data holders are required to do if
13 they're going to share information.

14 MS. HAN: Great. Thank you. So I think
15 several of you have touched a little bit on data
16 controls, and I wanted to plumb that a little bit
17 deeper. What are any additional data controls that
18 could be used to reduce the likelihood of re-
19 identification and how effective are those controls
20 and what are ways of measuring their efficacy?

21 And perhaps, Aoife, I will direct this to
22 you in the first instance. Thanks.

23 MS. SEXTON: Sure. Thank you. Yeah, so
24 first of all, I think in order to look at the
25 controls, I think you have to look at the risk of re-

1 identification, and they will obviously then inform
2 what are the level and the robustness of the controls
3 you need. So clearly, if it's a release of a public
4 data set, then the controls you're looking at will be
5 a higher degree of controls versus perhaps data that's
6 just being released intragroup, or as in the case of
7 Tr ata, is it a public release of data but just back
8 to a customer in an aggregated form?

9 Again, if it's role-level data, you're
10 looking at, again, what is the risk of re-
11 identification. So it is very contextual. So the
12 first thing you have to understand is the context of
13 the data itself and what's happening to the data, how
14 the data is going to be released and obviously the
15 sensitivity of the data. And that will inform you
16 then in terms of looking at some of the controls that
17 you might have.

18 Obviously, contractual controls are one of
19 the important things. And certainly in the case of
20 Tr ata, we have contracts with each of our customers.
21 And in that contract, we contractually prohibit the
22 customer from attempting to re-identify the data, and
23 we, ourselves, commit not to attempt to re-identify
24 the data. So that's one level of control for sure.

25 Obviously, the technical level of controls

1 are incredibly important. And this is where the real
2 expertise of the data scientists come in in order to
3 really look at what tools are available to them.
4 Jules mentioned homomorphic encryption, and that's an
5 encryption that's available to help with the security
6 of the data.

7 And, also, you're looking at differential
8 privacy. So there are new tools that are being
9 advanced that will help. So really the level of
10 sophistication of the data scientists will result in
11 the more robustness of the anonymization itself. It
12 is difficult to talk about audits because there isn't
13 a set threshold, even under the GDPR. There isn't a
14 sort of a threshold that says if you reach X,
15 therefore, you've definitely anonymized the data.

16 So from that point of view, it can be
17 difficult to look at, say, audits to ensure and to
18 specify that you have achieved the levels of
19 thresholds. But I do think that it is a combination
20 of the technical sophistication and expertise together
21 with the combination of safeguards, be it on the
22 contractual level, be it an organization security
23 level, having access controls in place, ensuring that
24 only people on a need-to-know basis can actually
25 access data.

1 And then in our case, obviously, we're an
2 independent third party. We are motivated to ensure
3 that we achieve a level of anonymization in a way
4 that's perhaps different than if you just have the
5 data in-house.

6 MR. POLONETSKY: I think it's important to
7 look at controls two ways. One is if this is a data
8 set that is statistical, and I want to ensure that
9 you're not going to attack it with trying to link in a
10 third party data set or the, like, clearly incredible
11 value. Controls are also what lets us look at the
12 pseudonymization that allows indirect identifiers, all
13 of the information that is actually the reason you
14 want data to be in some cases considered not
15 reasonably linkable because you've got structures in
16 place that don't allow the kind of linkage attack or
17 the other concerns.

18 Now, there's good pseudonymization and less
19 pseudonymization. GDPR's big mistake is it treats
20 them all the same. A minor pseudonymization where I
21 keep the data separately but, you know, clearly
22 haven't set up significant structural barriers is the
23 same on the GDPR as one where perhaps I put very
24 significant barriers in place.

25 I'd argue the FTC definition allows controls

1 to be used to guarantee, if you can, because you've
2 got the ability to limit what partners do with it, the
3 use of any of those indirect quasi-identifiers, the
4 data that is interesting, which hospital did this
5 happen into and so on and so forth, and allow you to
6 treat that, whether you call it pseudonymous or
7 protected pseudonymous or whatever you want to call
8 it.

9 We argued a lot about the labels often as
10 opposed to are there data sets where the risk is well
11 controlled and where there are attributes that
12 actually add to the precision that we can manage with
13 a combination of both technology and controls.

14 MS. JILLSON: I want to jump in with just
15 one last point. I'm sorry. I'll give you a chance to
16 respond to that as well.

17 So we've had a couple of questions from
18 the audience, and we just have a couple of minutes
19 remaining. The audience questions have pointed to
20 basically what can we do better. So Shane raised some
21 best practices around location data, but someone from
22 the audience raised the question of are these just
23 being adopted by a handful of companies, or, you know,
24 are these being more broadly adopted.

25 Another audience member asks about data uses

1 and if that should be taken more into account when
2 data is nominally de-identified but it results in an
3 adverse impact on someone.

4 So my question, my final question to you
5 all, is how can we do better. How can we think about
6 sensitive information in a more rigorous manner and
7 how can we use data controls in a different or more
8 effective manner so that this is a way to continue to
9 use and benefit data -- from data?

10 MR. WILEY: Well, to the first point, so
11 Cuebiq obviously is going out of its way to be
12 recognized as a privacy thought leader and is doing
13 the extra work, even as a small company, to create
14 these data sets, but we're also being very vocal about
15 it and being very open about our process and our
16 approach to it such that others that have at least in
17 this specific topic precise location data begin -- can
18 look at those techniques and adopt them themselves.

19 From a legal perspective, I actually agree
20 with Paul Ohm and others. I think sensitive data sets
21 like precise location data will require a higher duty
22 of care, and, again, just against the entire spectrum
23 of sensitive data. And so we would like to see that
24 come forward as well because I think that would then
25 be a forcing function for companies then to look to

1 apply more advanced standards internally.

2 MS. MCGRAW: I don't think you have to worry
3 as much about the companies that are doing the right
4 thing in this space and who -- you know, who come to
5 gatherings like this to talk about the -- you know,
6 how they're being super protective with the data,
7 right? It's how do you motivate the people who are
8 not talking about how well they protect data to get
9 them to actually protect data at that level.

10 And I think, you know, there's a combination
11 of, you know, the authorities the FTC already has, as
12 well as other authorities in the Federal Government,
13 but I -- you know, those need to be strengthened. And
14 I think, you know, in my opinion, the issue is
15 clearly before Congress to do much more than they have
16 done in the past on this issue, and I hope that they
17 do.

18 What I was trying to chime in on is
19 contractual controls, and, frankly, we use them and
20 we're subject to them, but they feel like CYA, weak
21 tea to me because once you get, you know, thousands
22 and thousands of contracts, how can you possibly go
23 out and chase those down? I would much prefer an
24 environment where whomever we give our users' data to,
25 with their consent but nevertheless knowing that

1 consent is not enough, that they are also bound by a
2 set of obligations to act ethically with respect to
3 that data, as opposed to me contractually making them
4 do it and then having to chase that down when they
5 don't.

6 MS. JILLSON: Well, thank you all. I'm
7 afraid we are out of time, but my thanks to all of the
8 panelists for a really interesting discussion.

9 And we will now take a lunch break. We'll
10 be back at 1:00 for another set of panels this
11 afternoon.

12 (Applause.)

13

14

15

16

17

18

19

20

21

22

23

24

25

1 REMARKS - NOAH JOSHUA PHILLIPS, COMMISSIONER

2 MR. TRILLING: Good afternoon, everyone,
3 and, no, I did not just raise the podium for myself
4 as people can probably figure out. Welcome back to
5 the afternoon session of the first day of our
6 privacy hearing. My name is Jim Trilling. I'm an
7 attorney in the FTC's Division of Privacy and
8 Identity Protection. This afternoon we will have a
9 panel discussion regarding consumer demands and
10 expectations for privacy and then a two-part panel
11 discussion that will compare and contrast current
12 approaches to privacy.

13 But first, before we begin the panels, we
14 are happy to have FTC Commissioner Noah Phillips here
15 to provide remarks. Commissioner Phillips joined the
16 Commission in 2018. He previously served as Chief
17 Counsel to Senator John Cornyn on the US Senate
18 Judiciary Committee. While working in the Senate from
19 2011 to 2018, he advised Senator Cornyn on legal and
20 policy matters in antitrust, constitutional law,
21 consumer privacy, fraud, and intellectual property.
22 He also previously worked in private practice as a
23 civil litigator.

24 With that brief introduction, it is my
25 privilege to turn the podium over to Commissioner

1 Phillips.

2 (Applause.)

3 COMMISSIONER PHILLIPS: The podium is still
4 not high enough. Story of my life. Thank you, Jim,
5 for that introduction, and more importantly, thanks to
6 the staff at OPP and DPIP and elsewhere for their
7 efforts putting together this hearing. Over the last
8 year, as I'm sure many of you know, we've had a lot of
9 really great hearings on a lot of really important
10 topics, but I would be hard pressed to identify, just
11 based on what I saw this morning watching from my
12 desk, a more substantive conversation that is more
13 needed right now, as I'll explain later. So really
14 congrats to all of you.

15 I have to start with the standard caveat.
16 What I'm going to say today, and as you will soon
17 realize, are my own thoughts and not necessarily the
18 thoughts of my fellow Commissioners or of the
19 Commission as a whole. These hearings, the ones
20 being conducted this week on the FTC's approach to
21 consumer privacy, reflect that we are in the midst of
22 a very robust national and even international debate
23 about consumer data privacy.

24 For those who've been studying and
25 advocating on these issues for years, many of whom are

1 with us today, I hope this is a welcome development.
2 I think it surely does reflect a great deal of
3 perseverance on your part. But for many policymakers,
4 for lawmakers, and for consumers, our consumer data
5 privacy moment seems in large part to have come out of
6 nowhere, and in a short time at that.

7 News events about large tech companies, data
8 breaches, politics here and in Europe, each and
9 together, too often leave this important debate to
10 skip right past the basic groundwork that I think we
11 need for a coherent policy discussion and from that a
12 coherent policy outcome.

13 Some people are freaked out, and in some
14 cases for good reason. Chairman Simons this morning
15 noted that privacy violations can result in real and
16 legally cognizable harms. But at core, the questions
17 we face and the answers that we choose will have broad
18 ramifications. So I'm concerned about how many have
19 been talking about consumer data privacy, and I think
20 you all should be, too. Whatever your views are, I
21 would hope we all agree that policy must be grounded
22 in informed debate.

23 So that's why I said at the beginning, the
24 hearings that we are holding this week are critical to
25 the national interest. And I'm particularly pleased

1 to see that they began today with a topic of the first
2 panel, a notionally modest but actually difficult and
3 essential step, defining the goals of consumer data
4 privacy.

5 As I have repeatedly said, including to the
6 Senate in discussing consumer data privacy, we need
7 first to distinguish between the operations of a
8 privacy enforcement regime and the underlying harms we
9 are trying to address. Too much of the discussion
10 here in Washington and in op ed pages has focused on
11 questions like whether the FTC needs penalty
12 authority, whether we need rulemaking authority,
13 whether we need more money. These are important
14 policy questions, don't get me wrong, but ultimately
15 they are derivative questions.

16 Rulemaking penalties, funding, these are
17 merely tools. It is the substance, the harms we are
18 addressing, and the rights that Congress intends to
19 create to address those harms that require our primary
20 attention. Privacy is a nebulous concept, and
21 different people can and do conceive quite differently
22 how individuals are harmed by a privacy violation.
23 They also differ whether and to what extent they
24 experience a given kind of conduct as a violation and
25 then how much they would pay to avoid it.

1 Are consumer data privacy harms limited to
2 physical injury and financial loss? Do they include
3 emotional distress? Is a sense of surveillance or
4 creepiness characteristic only of an eggshell
5 plaintiff, or is that something Congress needs to
6 prevent? What about a lack of empowerment or a loss
7 of control over data? And how, if at all, do these
8 things take us back to Brandeis' and Warren's famous
9 right to be let alone.

10 The decision as to which harms deserve
11 vindication by Congress is the predicate for deciding
12 how any law should look, including what liability
13 scheme we should adopt, what we permit, what we
14 prohibit and under what circumstances, and then and
15 only then what tools are appropriate for enforcing the
16 rights that Congress creates. To me at least, one
17 area of general agreement jumps out for action.

18 When the NTIA surveyed Americans in 2017,
19 the number one harm they reportedly feared, or we
20 reportedly feared, was identity theft. That makes
21 sense to me. And that is why I think the most
22 significant thing we can do for consumer data
23 privacy is to improve data security. While we often
24 discuss privacy and security disjunctively, they are,
25 in fact, close relatives. And all five FTC

1 Commissioners agree on the need for data security
2 legislation, including having the FTC's authority in
3 this area codified, providing us with civil penalty
4 authority to enhance deterrence and giving the
5 Commission jurisdiction over common carriers and
6 nonprofits. Moving that legislation forward would be
7 a major win for consumers and a major accomplishment
8 for privacy.

9 To go beyond this area of agreement, as I
10 said earlier, this week's hearings are critical. We
11 are asking the basic questions we need to ask about
12 what we should remedy and then considering real
13 questions about how the regime ought to look -- the
14 roles of notice and choice, access, deletion,
15 correction, and accountability. The order of these
16 conversations, not to mention the conversations
17 themselves, is essential, and the nation and Congress
18 ought to follow them.

19 I focused in my remarks today and elsewhere
20 a lot on Congress, and that is not by accident. Some
21 months ago, I was invited to address the Privacy
22 Coalition at EPIC's offices and answer questions.
23 After I gave a similar spiel about the need first to
24 agree upon privacy harms that we would address, a
25 participant asked me why I was focusing on harms and

1 not rights. That is a great question. And the answer
2 cannot be more important.

3 Unlike, say, in Europe, here in the United
4 States, there is no basic right to consumer data
5 privacy, or at least not yet. Political philosophers
6 locate the source of rights in God, in nature, in our
7 emergence from the state of nature, or maybe stemming
8 from some sort of Kantian reason. As a practical and
9 legal matter, however, rights flow either from the
10 Constitution or the laws Congress makes pursuant to
11 it. The mere fact that I believe I have a right to
12 something doesn't mean that I do. That is what the
13 role of the democratic process is.

14 Congress has, in fact, created consumer
15 privacy rights, including ones that apply to data. We
16 presently have a risk-based model where we sensibly
17 guard more jealously information the disclosure of
18 which concerns us more. And Congress may, as we are
19 now all discussing, create more general rights
20 regarding consumer data privacy.

21 But this is precisely the point. Congress
22 needs to make those rights. The framers of our
23 Constitution, who established a republican form of
24 government that has lasted for centuries and that
25 remains today a symbol of liberty and economic success

1 the world over, relied heavily for inspiration on the
2 philosopher John Locke. In 1690, Locke famously wrote
3 -- this is a quote -- "The power of the legislative,
4 being derived from the people by a positive voluntary
5 grant and institution, can be no other than what the
6 positive grant conveyed, which being only to make
7 laws, and not to make legislators, the legislative can
8 have no power to transfer their authority of making
9 laws and place it in other hands."

10 Our elected representatives in Congress,
11 not an enforcement agency led by five unelected
12 officials, are vested with the responsibility to make
13 the fundamental value judgments that consumer data
14 privacy legislation requires. For these choices to
15 have legitimacy and authority, they must come from
16 Congress. Not only would delegating the FTC too much
17 rulemaking authority risk that legitimacy and
18 authority, it poses other risks as well.

19 I am concerned about the impact on the
20 market of a set of far-reaching rules that could morph
21 with electoral politics. Businesses, whether they
22 like a particular law or not, need certainty and
23 predictability so they can plan and make investments.
24 These are crucial for them and for our economy. If
25 substantial changes to the law are in the hands of

1 just five people, the chance the rules of the road
2 will change back and forth will, on its own, chill
3 economic growth. And I'll add to it. I don't think
4 it's particularly good for the agency to have to deal
5 with that on a regular basis.

6 Consider the consequences at stake here.
7 The collection, use, and monetization of data is
8 endemic in the economy. It is not just a few very
9 noticeable firms. My children talk to Siri, and
10 someday my toaster will talk to me. Well, what will
11 it tell me?

12 This data-driven economy has provided
13 incredible benefits to businesses and consumers. Even
14 as we are facing questions about the negative aspects
15 of that economic development, we need to make some
16 conscious decisions about tradeoffs, balance sometimes
17 competing goals, and develop good policy on the future
18 of consumer data privacy.

19 Think about the regulatory advantages
20 held by large corporations and the impact of
21 regulation on competition. A new set of rules has
22 the potential to entrench the largest incumbents who
23 are best able to navigate and finance compliance
24 while posing substantial barriers to entry for
25 smaller players, even as those rules further some

1 privacy goals.

2 Consider for instance data portability, a
3 mechanism that many hope will facility competition. I
4 share that hope. Last week, Isabelle de Silva, the
5 President of the French Merger Authority, told folks
6 assembled at spring meeting about complaints she was
7 hearing from French startups that data portability in
8 the GDPR was enabling big companies to take their
9 customers. We have to consider that.

10 And this brings me to my next point. As
11 I've said, any consumer data privacy law will involve
12 tradeoffs. And to be clear, they may be worth it, but
13 we should make those decisions in an informed and
14 honest manner and, where possible, achieve an optimal
15 balance among different priorities -- competition and
16 consumer protection in particular.

17 We and Congress should be data-driven and
18 thoughtful, using existing research and commissioning
19 new research when necessary. That means, among other
20 things, taking the lessons we are learning from the
21 impact of GDPR and applying them to our policy
22 framework.

23 I want to end on what for me is a critical
24 point. We, as a society, are undergoing a major
25 shift in how commerce is conducted. And however

1 uncomfortable that may make some of us, it's not going
2 to go away. We're not going to succeed like the
3 samurai of old in keeping the guns off the island.
4 And by the way, that didn't ultimately work for them.
5 And no matter what laws Congress passes, in a sense,
6 they will never be enough.

7 Prescriptive rules in law enforcement
8 only go so far, especially without tradeoffs that
9 many do not want. To deal with what some have taken
10 to calling the fourth industrial revolution,
11 consumers and businesses, not just government, must
12 play a role. Laws alone are not going to inculcate
13 a sense of responsibility with regard to data,
14 unethical perspective, or a mentality of privacy by
15 design.

16 To accomplish this more fundamental shift in
17 behavior and thinking, which can do more than any law
18 enforcement agency with its limited resources can do
19 to protect consumer privacy, we need to encourage
20 companies across our economy and around the world to
21 view consumer privacy as a core value, as a business
22 differentiator for industry, and, most of all, we need
23 to encourage consumers to take their own privacy
24 seriously.

25 So here's my pitch. The discussion about

1 consumer data privacy is one of the most complex
2 policy debates we have had for a while. Likely with
3 dramatic economic, political, and social consequences.
4 There may be no do-overs if we get it wrong. So
5 let's go forward deliberately and carefully, taking
6 short-term wins where the consensus is clear, as in
7 data security, and making sure we are evaluating any
8 new privacy regime with data and careful analysis.
9 And let's work on developing a shared framework that
10 helps consumers and businesses understand the value
11 of consumer privacy so that any consumer data
12 privacy legislation is built on that framework of
13 shared values and a recognition of the importance
14 of privacy.

15 Laws work best when they reflect fully
16 shared values. That's from Aristotle, and I don't
17 know if the Professor Ohm is still in the room, but
18 that is, quite literally, antiquated. But it's still
19 true, and it's really important.

20 These hearings are a great example of the
21 discussions that I think we need to have -- maybe the
22 best example. So to those of you in this room and to
23 those at home who are watching, to people who have
24 submitted comments or otherwise engaged, I want to say
25 thank. Thank you for engaging and debating, for

1 putting meat on the bones of this privacy debate. And
2 I look forward to learning from you now and in the
3 future. Thanks very much.

4 (Applause.)

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 CONSUMER DEMAND AND EXPECTATIONS FOR PRIVACY

2 MS. VANDRUFF: Well, good afternoon. And
3 thank you to Commissioner Phillips for his remarks.
4 My name is Laura Vandruff. I'm an attorney in the
5 Division of Privacy and Identity Protection, and I'm
6 joined by my colleague, Dan Gilman in the Office of
7 Policy Planning. And we are here with the first panel
8 of the afternoon regarding consumer demand and
9 expectations for privacy.

10 I'd like to introduce my panelists with very
11 short bios. The longer versions are in your packet.
12 To my left is Professor Lorrie Faith Cranor, Professor
13 of Computer Science, Engineering, and Public Policy at
14 Carnegie Mellon University. Immediately to her left
15 is Avi Goldfarb, Professor of Marketing in the Rotman?

16 MR. GOLDFARB: Rotman.

17 MS. VANDRUFF: Rotman, excuse me, Chair in
18 AI and Healthcare at the University of Toronto.
19 Beside Professor Goldfarb is Ariel Fox Johnson, who is
20 Senior Counsel of Policy and Privacy at Common Sense.
21 Beside Ariel is Jason Kint, CEO of Digital Content
22 Next. Next to Jason is Laura Pirri, Senior Counsel --
23 excuse me, Senior Legal Director and Data Protection
24 Officer at Fitbit. And last but not least is Heather
25 west, who is Senior Policy Manager at Mozilla.

1 During our panel today, a number of my
2 colleagues -- at least one of my colleagues -- will be
3 in the room distributing comment cards. If you have a
4 question or if anyone in our web audience has a
5 question you can tweet it at us and we would be
6 pleased to try to integrate that. Those questions
7 will be moderated through Dan and me.

8 So, Dan, would you like to kick us off?

9 MR. GILMAN: Sure, thanks. So I'll start
10 with a very broad policy question, some would say
11 overbroad, but maybe we can unpack it a little bit and
12 then unpack it in the course of the discussion. So
13 the simple version of this is are consumer
14 expectations and demands relevant to creating policy
15 regarding privacy. So you could push for yes or no,
16 but you could also perhaps push for a version of when
17 and to what extent what might be some policy
18 substitutes or complements and enrich that a little
19 bit. So that's a question. I'd like to start with
20 Laura, if I can, and then have it open to the entire
21 panel.

22 MS. PIRRI: Sure. Hello and good afternoon,
23 everyone. So are consumer expectations and demands
24 relevant to privacy policy? I will say yes,
25 absolutely. And I think that in discussing what

1 customers and consumers want regarding privacy, it's
2 important to say that companies are very motivated to
3 understand their customers' expectations regarding
4 privacy so that they can deliver on them. And this is
5 not just because privacy generates customer trust and
6 goodwill but because it is good for business.

7 Sometimes when we talk about privacy and
8 companies' approaches to privacy, it is assumed that
9 privacy is somehow different from other product
10 attributes like the design of the product, the style
11 of the product features, the product quality. And, in
12 fact, that is not the case. Companies are constantly
13 assessing and responding to their customers' demands
14 for privacy in the same way that they do for other
15 product attributes.

16 And I can give one specific Fitbit example
17 around this. And for those of you who are not
18 familiar with Fitbit, we provide hardware, software,
19 and services that give our customers more insight into
20 their health and fitness. They purchase our Fitbit
21 devices precisely so that they can collect certain
22 activity information, including their steps and their
23 sleep, their heart rate, their exercise maps, their
24 food intake, and more.

25 And we have a Fitbit app that shows our

1 customers this information with a series of dashboards
2 and data visualizations. So from early on in our
3 company's history, we understood that our customers
4 wanted the ability to take their information outside
5 of the Fitbit app. They want to create their own
6 custom visualizations, and they wanted insights about
7 their data from data sets that were collected and
8 generated by multiple apps and services that they use,
9 so, for example, other nutrition or exercise apps.

10 In short, they wanted what we know as data
11 portability. So data portability became an early
12 tenet for Fitbit. And this is reflected in the early
13 coding models that are cofounders, our CEO James Park
14 and CTO Eric Friedman put together. These models
15 reflected that our customers' data should be easily
16 exported through an API. And, in fact, in early 2011,
17 not long after we launched our first device, about a
18 year after the first device, the Fitbit device was
19 introduced, we launched an API that enabled our users
20 to extend the uses of their data.

21 And not long after that, we launched a data
22 export tool that allowed people to download their data
23 directly from the Fitbit website. So I mention all
24 this to stress that this was in 2011. We launched our
25 data export feature globally. This is well before we

1 considered the GDPR or any data protection right to
2 data portability. We did this to satisfy a consumer
3 need and a demand that we saw within our user
4 community. We did this for business purposes rather
5 than for any regulatory requirement.

6 And I'll say that to this day, even now with
7 the GDPR in effect, we continue to consider our
8 consumer expectations first and foremost ahead of the
9 regulatory requirements. So for example, last year,
10 we gathered feedback from our customers about how
11 they're using our data export tool, and we found that
12 they're using it for many reasons, including to
13 download their information to share it with their
14 doctors, with their nutritionists, with their physical
15 therapists and trainers.

16 We also learned that for some of our
17 customers, the fact that we had this data export
18 feature was a competitive differentiator for us. We
19 had some customers who purchased a Fitbit precisely
20 because we had this data export tool. And this was
21 important validation for us of our early decision to
22 take consumer expectations regarding privacy into
23 consideration when developing our products and
24 deciding how we process our users' personal
25 information. So to answer your question, yes.

1 MR. GILMAN: Thanks, Laura.

2 Anybody else on this or a different version
3 of this?

4 MS. WEST: I'll pipe up. So at Mozilla, we
5 have a very similar approach to developing products.
6 We make Firefox, which is a browser, also known as a
7 user agent, which means at the end of the day, we want
8 to do what our users want us to do, and oftentimes
9 that means protecting their privacy because we live in
10 this world where people are starting to get worried.
11 And worried users aren't good for business, for sure.

12 You know, it's coincidence, but I happen to
13 have a Fitbit strapped to my arm because I trust
14 Fitbit and I find the service useful. And that means
15 that I am open to this idea that all of this data is
16 being, you know, processed.

17 I think that, you know, when we are
18 designing Firefox and when we're designing the other
19 Mozilla products that we are thinking about, we are
20 doing user research and we're thinking about what
21 those expectations look like. And I think from a
22 policy perspective, we need to be doing the same thing
23 because most of these problems can't be solved either
24 technically or with policy. It has to be a marriage
25 of the two.

1 And our top privacy principle when we're
2 designing products is don't surprise the users. And I
3 think that when we can translate that into policy and
4 start building product and policy broadly, for
5 Americans who don't want to be surprised but do want
6 to use these amazing, cool tools, we start to look at
7 the right answer.

8 So I also agree. I think that consumer
9 expectations really do need to inform the policy as
10 well.

11 MR. GILMAN: Lorrie, you wanted to --

12 MS. CRANOR: Yeah, so I agree that consumer
13 expectations and demands are relevant, but I think the
14 question comes up as to how do we know what consumer
15 expectations and demands actually are. And we see
16 some companies that I think probably do have a pretty
17 good pulse on what their users want, but there are
18 others that maybe don't. And I think part of it
19 depends on how you frame the question, what kind of
20 answers you get.

21 And so I don't know that we can -- you know,
22 when a company says, oh, well, you know, my customers
23 are happy to give me their data or they want
24 advertising, they want targeted advertising, I think
25 you have to look with some skepticism about how are

1 they measuring this, how are they framing the research
2 question and who collected that data.

3 MS. VANDRUFF: So Lorrie, that's a good
4 segue. We're going to unpack a lot of that on this
5 panel. But let's just take a piece of that, and I'd
6 like to ask the question first of Ariel. How do
7 consumers' privacy expectations and demands vary, in
8 particular across consumers?

9 MS. JOHNSON: Sure, and thank you for having
10 me today. At Common Sense, we focus a lot on kids and
11 teens. And I think they have very different
12 expectations and demands than adults do, and they're
13 an important population to look at because I think
14 something like one in three users on the internet
15 worldwide is under 18. And you know, parents have a
16 lot of expectations for their kids and teens, also.
17 Parents have a lot more expectations that their
18 children will be protected and their information
19 protected online.

20 Unfortunately, some of this is -- some of
21 this is because of COPPA, which is great, and then
22 some of this is people don't understand COPPA and they
23 think it prevents the collection of any information
24 from children under 13 or even under 18. But kids,
25 they don't really have an expectation of privacy, and

1 they don't really have an understanding of privacy.
2 They don't know that a toy that they talk to is
3 recording them or sending their voice or information
4 somewhere. They may view -- in studies they have
5 viewed GPS and location tracking on devices as sort of
6 a positive thing. And unlike adults, who I think in
7 this past year really woke up and started to better
8 understand what happened with data and how things
9 worked behind the scenes that privacy is more than
10 just, you know, targeted ads, children are not going
11 to have that kind of a wake-up call. And so we need
12 to, I think, work to make sure that they are
13 protected, whether that is their expectation or desire
14 or not.

15 And teens are also a different population.
16 Unlike children, I think teens want privacy. Everyone
17 agrees they want privacy, and maybe we just disagree
18 about if they want privacy more from their parents or
19 from a faceless company. But, you know, in our Common
20 Sense polling, 86 percent of parents, 79 percent of
21 teens, they've all adjusted their privacy settings.
22 97 percent of parents, 93 percent of teens thinks it's
23 important that sites get permission before sharing or
24 selling data.

25 I mean, the numbers are slightly higher for

1 parents, but they're still quite high for teens.
2 Teens express an interest in having privacy, and I
3 think they just maybe don't know how to protect it.
4 One number that was quite different for adults and
5 teens, as I think that adults were maybe -- or teens
6 were twice as likely to never read privacy policies, I
7 think that makes a lot of sense. It's very rational
8 if an adult doesn't understand a privacy policy, you
9 know, good luck to the 13-year-old.

10 So we see what their expectations are and
11 whether they're being met by some companies or whether
12 the teenager feels like they don't have any ability to
13 do anything about it. I don't know, I think some
14 companies are meeting consumer demand for privacy and
15 sometimes consumers have an expectation of privacy,
16 but they are resigned to the fact that they may not
17 get it, and we might see that a lot more with
18 teenagers.

19 MS. VANDRUFF: So, Jason, I just want to
20 follow up. Ariel's provided a good description of
21 where children and parents fall in the spectrum.
22 What's the perspective of publishers with respect to
23 how privacy expectation and demands may vary across
24 different populations?

25 MR. KINT: Sure. Thank you for having me.

1 And to reiterate, I think there are some really
2 important data points from Ariel. There's a myth out
3 there that younger people don't care about privacy,
4 and it's quite the myth, so I'm glad you popped that
5 with some stats.

6 So regarding publishers, you know, the thing
7 we worry most about is protecting that direct
8 relationship that we have with our audiences. I
9 represent DCN, and all of our members, that's what
10 they have is a direct trust relationship with their
11 users and their advertisers. They're brands you know
12 like The New York Times and CBS, ESPN, NPR, and their
13 relationship is built off of that meeting consumer
14 expectations.

15 Michelle Richardson earlier today from CDT
16 very much focused on this goal of maximizing the trust
17 in that relationship with the user. That's what we're
18 trying to do, and most of the problems out there,
19 particularly consumer expectations, have to do with
20 secondary uses of data. And that's what we see as
21 publishers, too. There are certainly companies that
22 publishers work with to deliver on the exact product
23 that the user wants, the service that they're trying
24 to experience, but when the data is used for other
25 purposes -- that's why purpose limitations are so

1 important -- when they're used for other purposes
2 outside of the user's expectations, it erodes trust.

3 We are here today, we're doing these series
4 of hearings because there is an erosion of trust in
5 digital right now, and it comes from very significant
6 things that happened outside of consumer expectations.
7 We have tried to measure those expectations through
8 surveys and research. It's important to note that the
9 two companies that collect and use data more than any
10 companies in the advertising business, Google and
11 Facebook, they collect data on a majority of the pages
12 on the web. Facebook collects data across over 8
13 million publishers sites. They've disclosed that.
14 Google on over 70 percent of the top 1 million sites.

15 We've asked users, do you expect -- we've
16 done this for both companies -- do you expect your
17 data to be used for targeted advertising across the
18 web, across multiple contexts. Two out of three users
19 say no, they do not expect that to be happening. So
20 that is a very significant part of the concern that is
21 eroding trust in the marketplace, and we need to
22 restore that value back to the publishers with the
23 direct relationship with the user.

24 MR. GILMAN: Thanks. I wonder if some of
25 the other panelists can sort of follow up on this

1 issue that Jason mentioned, and that is how we assess
2 or measure consumer expectations and consumer demands.
3 Obviously, consumers make certain choices in response
4 to offerings. We do various kinds of surveys which
5 may raise other issues, but there's both sort of what
6 are the background expectations, what do policies
7 mean, what are their preferences. What are some of
8 the different ways we assess the expectations and
9 demand more or less reliable or persuasive in
10 different contexts? Can we get into this sort of
11 assessment a little more?

12 MS. PIRRI: I can speak to how companies
13 both assess and address consumer expectations
14 regarding privacy in both the context of children as
15 well as sort of more generally with adults. So first
16 in the context of children, Ariel mentions the
17 standards that are set out by COPPA. In addition,
18 companies often look to good privacy-by-design
19 principles. And I can give another Fitbit example,
20 which is that we have an Ace device that is for kids.

21 Our market research showed that parents and
22 kids were looking for ways to encourage healthy habits
23 and to get kids to be more physically active,
24 including through reminders to move as well as step
25 competitions with friends and family. Our research

1 also found that parents were very concerned about how
2 their kids' personal data was being collected and
3 used.

4 So the approach that Fitbit took in
5 designing this device was to minimize the data that
6 was collected and used and to focus on the essential
7 functionality for the goal of encouraging kids to be
8 more physically active. So, for example, we do not
9 collect kids' email address. We do not collect their
10 last name, we do not collect their GPS location
11 information, and we do not collect their personal
12 profile photos.

13 We use the information solely to provide the
14 services. We do not use it for marketing. We do not
15 use it for third-party integrations. And in addition,
16 we give parents control over the requests to friend or
17 connect with their children on the platform.

18 The other subject I wanted to discuss, too,
19 was more broadly with adults and how do we assess
20 privacy expectations in general. And I think on this
21 point it is important to stress that privacy does not
22 necessarily mean private. Sometimes when we discuss
23 privacy, this is the underlying assumption. And at
24 Fitbit, we think about privacy as giving people
25 control over their information, control that we enable

1 through product features that allows people to make
2 different preferences regarding how their information
3 is used.

4 So the underlying assumption is not that
5 people's preferences are uniform but rather that they
6 differ, they do vary, and our role is to enable people
7 to express those different preferences. The social
8 features of our service reflect this approach. So
9 many of our users choose to share information with the
10 Fitbit community, which is a positive feedback loop
11 for encouraging healthy behaviors like eating well and
12 like physical activity.

13 Participating in the community is entirely
14 optional. For those who do participate, we give
15 granular choices around how they can share their
16 information. So, for example, some of our users
17 choose to share their daily activity or their daily
18 step count publically through Twitter. We have other
19 users who share that information with a more limited
20 audience with just their Fitbit friends. And we have
21 other users who choose to share other information like
22 the graphs of their weight and sleep over time.

23 So while some --

24 MR. GILMAN: I'm sorry, Laura. This is
25 important, I think, and we want to hear more about it.

1 MS. PIRRI: Okay, let me just get to the
2 bottom line.

3 MR. GILMAN: But if you could wrap up, I'd
4 like to hear from some other panelists, too.

5 MS. PIRRI: Yeah, yeah. So, I mean, the
6 bottom line is that we address our customers'
7 privacy preferences by giving them choice and by
8 giving them through sensible defaults, where almost
9 all information is defaulted to private. And then we
10 have granular choices so that people can choose to
11 share the information that they want while others can
12 decide to keep it private.

13 MR. GILMAN: Thanks, thanks.

14 MR. GILMAN: Avi.

15 MR. GOLDFARB: So, Dan, I think you asked
16 originally about measurement and how do we think about
17 measuring preferences. And in some sense, measuring
18 privacy preferences isn't different from measuring
19 other kinds of preferences. Just like Laura, you
20 know, she opened with privacy is an attribute and
21 there are other attributes. And so, broadly speaking,
22 in economics at least, when we think about measuring
23 preferences, we think about two different strategies.

24 The first one is you can ask people what
25 their preferences are. And if you ask people what

1 their preferences are, they tend to like things that
2 sound good, like privacy and like openness. And on
3 the same topic, you could ask the same question, hey,
4 do you think privacy here is good; they'll say yes.
5 Do you think openness here is good; they'll say yes,
6 even though in some sense those can be the opposites.

7 The other way to measure is to reveal
8 preference, which is where you observe what people
9 actually do, particularly in the context of real
10 tradeoffs. And, generally, that tends to be much more
11 powerful. So the question is, when people are
12 informed -- that's an important caveat -- when people
13 are informed and they continue to use the services of
14 a company, even though there's been very public
15 privacy violations, does that tell you something about
16 their underlying preferences for privacy relative to
17 the other attributes that that service provides?

18 MS. JOHNSON: So briefly, I guess, I think
19 it's a really important caveat if people are informed
20 and then also if they choose to use the service
21 because I think in a lot of contexts, particularly
22 let's talk about children again and teens and they're
23 in school, you have to use certain services to get an
24 education or you have to use certain services for your
25 work.

1 I know people are trying to see, you know,
2 how long they can avoid Google. You know, I couldn't
3 have my job and not use Gmail. So in a lot of these
4 instances, I don't know that we can really see both
5 information and a choice by consumers.

6 Also, just really quickly with respect to
7 teens and what they do and what they might say they
8 want and then what they persist in doing, you know,
9 their brains are still developing. Their prefrontal
10 cortex is not developing. They're very risky,
11 they're, you know, more likely to have some sort of
12 fatal accident, so it's not just, you know, risky in
13 terms of privacy behavior. They're very reward-
14 sensitive. They want whatever quick thing they're
15 going to get now, and so they're going to share
16 information or click on that bright blinking button
17 and not think about the long-term consequences down
18 the road, which they might not be able to fully
19 understand and likely can't understand or even imagine
20 what they are.

21 And so I don't -- you know, they're going to
22 self-reveal before they self-reflect, and so they're
23 sort of making a choice in that instance. I thought
24 Professor Ohm did a good job talking about if it was a
25 real choice and this question of dark patterns, but I

1 don't know that I put a lot of stock in what they
2 might be doing online and whether they really have
3 choices.

4 MS. VANDRUFF: Can I just put a slightly
5 finer point on it? And, Lorrie, I'd like to ask you
6 this question first. At the outset of today's
7 session, there was a robust discussion about the so-
8 called privacy paradox, and there's been a lot of
9 literature about this, and, Avi, you talked -- you
10 alluded to it just now in your remarks. So I guess
11 what I'd like to throw to the panel and to Lorrie
12 first is whether there exists a privacy paradox. Is
13 that the right way to frame it, and what does that
14 mean for assessing consumer demand and expectations
15 for privacy?

16 MS. CRANOR: Yeah, so I agree with the
17 panelist this morning who said that there probably
18 isn't really a privacy paradox, that, you know, we see
19 behavior that on the surface appears contradictory,
20 but when you dig deeper into it, you can see that
21 people are making decisions, but it's not based on
22 full information. And they may not have a robust set
23 of choices that they can decide between.

24 So I actually did research at this point
25 about 10 years ago with Alessandro Acquisti and some

1 of our students, where we said, well, what if we could
2 really show people in a very easy way what their
3 privacy choices are when they're shopping online. And
4 so we built a search engine that had a privacy meter
5 in the search results, and so you could see it at a
6 glance. And we gave people money and we asked them to
7 go shopping online and they got to keep the change.
8 And we set it up so that they could shop at the more
9 expensive website to have better privacy or shop at
10 the cheaper website, get the exact same item but with
11 worse privacy.

12 And we found that when you set it up so it's
13 so obvious which is better and which is worse, people
14 actually will pay a little bit more to shop at the
15 site with better privacy. But all you have to do is
16 move those meters into the webpage itself instead of
17 in the search engine and the effect goes away. So
18 that little bit of extra burden of having to go and
19 find out about privacy is too much.

20 MR. GILMAN: So what's the response there,
21 right? We prefer revealed preference, all things
22 equal, as Avi pointed out. Information is limited,
23 imperfect. Choices are limited, and not to imply that
24 we ought to be sanguine about these limitations, but,
25 you know, in some ways decision under uncertainty is

1 ubiquitous. The market may provide a few choices.
2 There are many choices, but not infinitely many
3 choices.

4 What do we do -- I thought you raised an
5 interesting point in contrasting, you know, two models
6 of the experiment. One was the search engine and the
7 other was the webpage. What do we do to get a sense
8 of what really matters to consumers given these
9 limitations?

10 MS. CRANOR: Yeah, so I think, you know,
11 revealed preferences definitely gives you a lot of
12 good information, but you have to realize the whole
13 context. You know, this is very contextual and just
14 because a particular company does something and you
15 don't see their customers fleeing doesn't mean that
16 their customers were happy with what the company did.

17 I think you have to look at the whole thing,
18 and I think the research needs to be a combination of
19 these natural experiments that occur, as well as some
20 explicit lab experiments or online experiments where
21 you can control the conditions and see which are the
22 factors that are driving things.

23 MR. GOLDFARB: So first I want to say that
24 Lorrie and Alessandro's study is, you know, in some
25 sense, exactly where we like to be in the sense that

1 it was revealed preference and it showed a preference
2 of privacy under one situation and not the other. At
3 least my reading of the paper, it's not obvious which
4 was the right one, but that difference is interesting.

5 But I do think, circling back, it's
6 important to remember that privacy is one attribute
7 among many, and one thing that we need to think about
8 very carefully is how much we want to elevate that
9 attribute above the others versus not. And related to
10 that, it's important to remember that privacy is a
11 beneficial attribute, but it's like other attributes
12 when you're designing a product, you have these
13 tradeoffs in the sense that search engines tend to be
14 more useful when they can take advantage of data.

15 And social media platform tends to be more
16 useful if data gets shared within the platform. So,
17 you know, there's certainly places where the costs of
18 privacy are relatively high compared to what the
19 consumer benefit would be, and I think that's what
20 everyone else has been talking about, but I think it's
21 really important to recognize there are tradeoffs
22 here, the data is useful, and so in -- you know, in
23 product design, with or without regulation, those
24 tradeoffs should be at the forefront.

25 MR. GILMAN: Okay. Thanks. Should we move

1 along? I think this is very good, and I hope
2 panelists will follow up with us after. I know you
3 all have a lot of work on this. I don't mean to short
4 change anybody.

5 So I guess we've got twin questions about
6 practices that do and don't meet consumer expectations
7 to the extent we know them. One, do practices that
8 fail to meet consumer expectations either necessarily
9 or typically lead to consumer harm? And maybe then
10 we're going to want to ask whether, to what extent,
11 and when firms are responsive to consumer demand for
12 privacy.

13 So maybe with the first one we could start
14 with Ariel but then open it up to the panel.

15 MS. JOHNSON: Sure. I think that if
16 consumers are -- and I guess we'll take out really
17 small children who I don't think, you know, know that
18 they don't have an expectation of privacy, and so
19 meeting that, I don't know that that's a great thing.
20 But in general, I think if a consumer is surprised or
21 confused, didn't expect what was going to happen to
22 happen, that that's a bad thing.

23 I do feel that there are also times when a
24 consumer has expectations that they have no control
25 and that expectation is met and that can also be a bad

1 thing, so it's not just when consumer expectations
2 aren't met that there's harm. But if they wouldn't
3 have done what they did, had they known what you would
4 do with their information or their data, that seems
5 like a harm to me.

6 MR. GILMAN: How about the question about
7 consumer demand? Maybe Avi, Jason, Laura, any
8 thoughts on how or to what extent firms are responding
9 to consumer demand?

10 MS. PIRRI: Yeah, I'm happy to speak to
11 consumer demand. And my points are actually very
12 relevant to Lorrie's point about the relevance of
13 privacy at the point of making a selection about which
14 products to use, as well as to Avi's point that, you
15 know, privacy is one consideration that customers
16 consider amongst many.

17 And so on the purchasing point, I will say
18 that one way that Fitbit has been responsive to
19 consumer demand is in how we market our devices. We
20 understand that the data that our devices collect and
21 the functionality that they provide are relevant
22 considerations at the time of purchase. So our
23 website provides information about the different
24 devices that they -- the devices that we, the
25 different data types that they collect, and the

1 different functionality that they provide.

2 So this ranges from, you know, basic step
3 count, sleep tracking, to more sophisticated features
4 like heart rate and GPS tracking. And consumers may
5 choose to purchase a device that has more limited data
6 collection; however, this means that there may be a
7 tradeoff in that there is also more limited
8 functionality. So our devices that do not collect
9 heart rate data or GPS data don't have certain --
10 don't enable certain features like the heart rate
11 information and the dashboard or the exercise and run
12 maps that are based on GPS data.

13 Also, some of their metrics may be less
14 accurate like the distance that they travel, the
15 calories that they burned, their sleep stages. So
16 these are important factors in the purchasing
17 decision, and there are definitely differences
18 in the product experience that come from these
19 considerations. And the approach that we've taken at
20 Fitbit is to be transparent about this and to empower
21 our customers to decide what is the right tradeoff
22 from them based on the product comparison information
23 at the point of purchase.

24 MR. GILMAN: Thanks.

25 Jason, I know you'd been trying to get in

1 the last question. I don't know if you have --

2 MR. KINT: Sure. I'll keep it simple that I
3 think that are the demands being met, no; and
4 expectations are going down to what I think Ariel said
5 is a problem. And so that's not a good thing when
6 expectations are going down, you want them to go up.
7 And there is an intersection that we'll get into
8 around competition that's a very large discussion
9 right now across our industry that's really important.

10 You know, Avi said search engines, plural,
11 which I always find a bit amusing. So there is not
12 the same sort of choice we should have, and so we are
13 forced into certain products, you know, in a world
14 where there's really good competition around certain
15 types of experiences, for instance, maps.

16 Certainly if you put your data or Google
17 Maps is using your data for the purpose of delivering
18 directions, you would expect that and you would
19 appreciate that and that's a fine product experience.
20 It's when the data is again used for a secondary
21 purpose which you wouldn't expect and you don't really
22 have control over that it becomes problematic.

23 Most of our 80 or so premium publisher
24 members do things with data as part of the experience
25 that most consumers fully expect. And if they violate

1 that, they'll go somewhere else, they have that
2 choice. The New York Times or The Wall Street Journal
3 certainly I think most people want them to recognize
4 you when you come in as a subscriber so that you can
5 actually immediately consume the news and not have to
6 log in every time. But if they violate that data
7 relationship, then you will go somewhere else because
8 there's real competition in the news category, for
9 sure, and there's certainly competition in the
10 entertainment category.

11 And so for each of those cases, what you
12 do with the data as a direct consumer experience has
13 to align with preserving and maximizing that
14 relationship. If it's used for other purposes, which
15 you don't expect, then it becomes problematic, and
16 big, behemoth companies that are all intertwined in
17 our lives don't have those same sort of restrictions.

18 MR. GILMAN: Avi, you were trying to --

19 MR. GOLDFARB: So I'm listening here, I'm
20 trying to figure out where the -- think through where
21 the market failure is in the sense that, you know,
22 yes, consumer negative surprises, that's bad for sure.
23 That's bad for firms, that's bad for consumers. But
24 we have some sense that firms do respond. We just,
25 you know, heard how Fitbit thinks about these, and

1 lots of other companies, I'm sure if they were up
2 here, would say the same thing.

3 And so the question is, why aren't -- you
4 know, there's some sense at least on others on the
5 panel that they're not responding enough. And the
6 question is why aren't they responding enough. Does
7 that have to do with privacy policy, per se, or, you
8 know, Jason seems to be hinting, I don't want to put
9 words in your mouth, that it was more about antitrust
10 policy than privacy policy in the sense that there
11 wasn't choice. And it's not -- you know, if there's
12 choice, if there's lots of competition, then we're not
13 so worried about privacy because you can go elsewhere
14 and we can think about revealed preference.

15 But if there's no choice, then privacy
16 becomes more important. So this, you know, thinking
17 through where the market failure is given that
18 privacy's one attribute among many I think is very
19 important.

20 MR. KINT : Totally agree. I just want to
21 lock in on one point there. It is the intersection of
22 data policy and competition that we think is critical.
23 And I think Facebook has a company to outline this,
24 and there's a great research paper that was put out on
25 this, is a great case study on a company that led with

1 privacy for its first five or six years as a company.
2 You couldn't even use the product unless you were
3 doing an experience that was very privacy protected.
4 The executives all talked about privacy as the most
5 important thing to the product.

6 Once it got to a certain size and certain
7 public expectations when it went public, it started to
8 lower the bar on a lot of its decisions, and the
9 quality of the product went down but was okay because
10 they were a certain size. And we've seen what's
11 happened now over the last few years.

12 MR. GILMAN: Maybe Lorrie and then we should
13 move on.

14 MS. CRANOR: So I think there are many
15 products where it's actually really difficult to even
16 find out the choices. We're doing some research right
17 now on IOT devices, and consumers are telling us that
18 they have no idea how to figure out what data their
19 IOT devices are collecting. And we've seen recently
20 that there have been cases where -- I think it was a
21 thermostat that was -- it was suddenly revealed had a
22 microphone in it.

23 Who would have thought their thermostat had
24 a microphone? Once you've bought it and put it on
25 your wall, it's actually not that easy to go buy

1 another one, take it down, and replace it. So I think
2 that there are many cases where consumers don't have
3 real privacy choice.

4 MS. VANDRUFF: Okay, so to just segue,
5 let's talk for a moment about the incentives, then,
6 for firms to respond to providing privacy, the
7 thermostat or otherwise. And moving out of the
8 thermostat market for just a moment, Heather, let me
9 throw a softball your way and ask you how browsers
10 respond to consumers' expectations and demands with
11 respect to privacy.

12 MS. WEST: Sure. Yeah, that is a softball.
13 I can talk about this one all day, but I'll try not
14 to.

15 MS. VANDRUFF: Okay.

16 MS. WEST: So as we move into this world
17 that is ever connected and as people understand some
18 of the data flows that are involved when they're, you
19 know, working online, watching TV, streaming services,
20 all of these things that we don't necessarily think of
21 as sending data off to third parties, you know, we
22 decided as the user agent, we needed to figure out
23 what our users wanted to do.

24 And so we did a bunch of research, and if
25 you wanted to search for that, it's called Improving

1 Privacy without Breaking the Web, and it goes through
2 our entire research process. What do people actually
3 want? What are some of the balancing factors that
4 they are interested in? Does this actually break
5 things?

6 And so we started to build the tools that we
7 saw demand for in that market. And some of those
8 tools are enhanced tracking protection, and we work
9 with partners to make sure that that doesn't, you
10 know, break unintended pieces of the web. No one's
11 asking for that. But also to create a gradient -- or
12 a spectrum of tools for our users so that if you
13 legitimately want to break everything that's not a
14 first party on a page, you can do that. I want you to
15 understand what that means. So we tried to make the
16 preferences clear, that's a hard problem. But we made
17 some other guesses about what kinds of preferences we
18 ought to be creating tools around.

19 And in the last year, we also created
20 something called Facebook Container, which I think is
21 actually a really interesting use case. And what it
22 does is it divorces your interactions on Facebook as a
23 first party with your interactions on pages that have
24 Facebook as a third party because what we heard from
25 our users is they were surprised that Firefox, their

1 browser, who is trying to protect them online, was
2 facilitating those data flows. And that's more of a
3 little bit of an experiment to see how that works and
4 how -- you know, whether people like it. People seem
5 to like it. But those are the kinds of tools that we
6 have been building and thinking about. And so we're
7 actually looking for people to give us some ideas
8 because we want to build those tools.

9 MS. VANDRUFF: And, Jason, similarly, how do
10 publishers balance expectations and demands with the
11 need to obtain metrics on their audience and
12 otherwise?

13 * MR. KINT: Yeah, I think that's -- metrics
14 is a perfect example where they do align with consumer
15 expectations, and the best thing we could do as an
16 industry is, you know, if a user is going into a
17 publisher's site and they're trying just to keep track
18 of how many people are on their site for the purpose
19 of measurement that we don't want to create friction
20 around that because that's fairly in line with first-
21 party expectations.

22 There's other things like fraud prevention,
23 billing that would fit in that category.
24 Personalization, if you go into a sports site, it
25 knows who your favorite sports teams are if you tell

1 it, things like that. Again, it's about the secondary
2 uses. The word "tracking" was used by Heather, which,
3 you know, I think Mozilla and Apple are both doing
4 brilliant work and thoughtful work to try to delineate
5 between these two experiences so that they don't break
6 things but at the same time give the consumer more of
7 what they expect. So I would like to see more
8 positive work there.

9 I think the only challenge to publishers
10 that is nuanced but is important to understand is that
11 an Apple Safari experience or a Mozilla Firefox
12 experience or any experience with tracking prevention
13 could be better for the user because that advertising
14 still has to compete with ads that are delivered in a
15 world of relentless ubiquitous tracking. Often the
16 ads that have all the data that can be coupled with
17 the ads on the open web with kind of this unbridled
18 ability to collect data and target, those ads end up
19 becoming more valuable because there's just more data
20 layered on.

21 That's only because of the way the market is
22 currently designed. If we raise the bar across the
23 entire industry equally, then we will solve for that
24 issue so we can have an experience like what Mozilla
25 and Apple are envisioning that's even better for the

1 user, and that's the tricky part and why the work
2 being done here is really important.

3 MR. GILMAN: Thanks. So, you know, several
4 of you have mentioned competitive dynamics, but also
5 Avi mentioned and then several people followed up with
6 the idea of tradeoffs, you know, nonprice factors of a
7 good or a service may be many. Even privacy itself
8 and privacy-pertinent features may be many and
9 complex.

10 So I wonder, maybe starting with Avi, but
11 then also others, Laura and Ariel, want to know about
12 some of these tradeoffs and whether, to what extent
13 firms incur opportunity costs as a result of increased
14 investments in privacy tools. I mean whether we're
15 talking about functionality, accessibility, ease of
16 use, innovation, security, et cetera. How does some
17 of this gets teased out.

18 MR. GOLDFARB: So at a high level, it should
19 come as no surprise that data's useful. The reason
20 companies are trying to collect data is not because
21 they are trying to violate privacy, per se, typically.
22 It's instead that the data that they have is useful --
23 that they could collect about consumers and others is
24 useful to the company. And so restriction, regulatory
25 restrictions in particular, on information flows are

1 going to restrict the ability of firms to do that.

2 That said, to the extent that consumers are
3 demanding it, that actually -- you know, that goes in
4 the other direction because if consumers trust firms
5 more then they are going to be willing to give those
6 companies potentially more useful data or just
7 generally be their customers, which is what the firm
8 is trying to achieve in the first place.

9 MR. GILMAN: Anyone else?

10 MR. KINT: I would just add that just to
11 reiterate what the cost from privacy rules can be when
12 friction's introduced to the user when things are
13 aligned with their expectations already. And so if
14 you're going to a website or an app, and lots of
15 people like to talk about the cookie banners in Europe
16 as if that's some new GDPR thing, but it's not, it's
17 from -- actually from pre-GDPR, and the intention is
18 to make those go away when they're not necessary. If
19 a user is going into a website and they're being hit
20 with notices as part of that experience and that
21 experience aligns with their expectations, then it's
22 just -- it's just adding friction and a cost.

23 And so I think that's actually where the
24 California law, and I know you had Alastair Mactaggart
25 earlier today, where it was really smart is it hasn't

1 gotten in the way of using the actual websites as you
2 would want to use them, and it hasn't gotten in the
3 way of behavioral advertising inside the context of
4 the website. It's preventing the ability to do
5 secondary uses of data when the user doesn't want
6 that, and that's smart.

7 MS. PIRRI: I will just add that there
8 absolutely are tradeoffs between functionality and
9 innovation on the one hand and privacy and security on
10 the other hand. The example that I gave of the
11 devices -- the Fitbit devices that we offer that
12 collect more data just have more functionality and
13 accuracy is one place where you see this, those kinds
14 of tradeoffs. But you see it also outside of the
15 product context just in terms of, you know, how data
16 can be used more generally for, you know, even social
17 good purposes, so for example in the, in the context
18 of health research.

19 Breakthroughs in health research often
20 come from amassing large data sets of very personal
21 and sensitive information from multiple data sources.
22 So, you know, obviously, there are significant
23 privacy considerations here. At the same time there
24 are social good considerations, you know, that
25 countervail. And the privacy protections that get put

1 in place or that tend to get put in place to protect
2 individuals, for example, getting individual consent
3 as well as aggregating or de-identifying data sets, do
4 mean that there are restrictions on those research
5 data sets and inevitably some useful data is removed
6 from those data sets, some useful data that could have
7 been used for a social good.

8 And as in the product context, in the
9 research context, I think it's all about striking the
10 right balance between privacy and the innovation that
11 can come and the insights that can come from data.
12 And the one point that I would stress, too, is that in
13 the research context there are multiple players, there
14 are usually multiple parties like, you know, academic
15 institutions, research organizations, government, and
16 privacy industry. And so it's not just about any one
17 organization striking the right balance but having
18 some consensus across the ecosystem about what that
19 right balance is.

20 MS. JOHNSON: And I think I might just say
21 that while I agree there are definitely sort of social
22 good uses of data and it's not all about the
23 individual, I think if we're remiss in not mentioning
24 that I think the flip side is also true that there are
25 negative externalities in terms of data being

1 collected. What might not be a big deal for one
2 person suddenly could be very problematic if we're
3 talking about a community or a country, and so it sort
4 of works both ways.

5 MS. VANDRUFF: So we're near the end of our
6 panel, and we received a terrific question from the
7 audience that is a good segue to the next couple of
8 panels which will address in different ways public
9 policy questions about sort of where we go from here.
10 So Dan and I would like to pose to this group a
11 question that marries or that provides a good bridge
12 between the issue of consumer demand and expectations
13 for privacy with the larger public policy question of
14 sort of what's next.

15 And the question is this: whether -- well,
16 what you would think of Congress passing a law that
17 would require heightened protection for data
18 collection and use that does not meet consumer
19 expectations. Is that a workable solution? Is it
20 good public policy?

21 MS. WEST: I think it's a very interesting
22 way to frame it, but, you know, Mozilla supports the
23 passage of legislation. We published a blueprint for
24 what we think that should look like and it does have a
25 lot to do with consumer expectations, and purpose

1 specification that Jason's been talking about is also
2 a big piece of that to talk about -- okay, so I gave
3 you my phone number but here's how I expected you to
4 use it. And I do think that that's a good start to
5 the discussion around how to translate these consumer
6 expectations and desires and preferences into
7 legislation or regulation.

8 MS. VANDRUFF: Anyone else?

9 MR. KINT: I would just -- you know, yes,
10 it's a good start, and I think I would then --
11 ultimately we'd recommend translating that into using
12 context as an important way to measure consumer
13 expectations as much as anything and putting purpose
14 limitations around that so that way it can be enforced
15 in a way that's material.

16 MS. JOHNSON: And I guess, you know, are we
17 talking about expectation, are we talking about demand
18 and desire? I'm concerned. Well, I agree it's a good
19 start, too. I think I don't just want to meet
20 consumers' currently probably pretty low expectations.

21 MR. KINT: It's a good point.

22 MR. GOLDFARB: So I also think it's an
23 intriguing idea. There are sort of two challenges I
24 can think of. One is not all consumers have the same
25 expectations. So I think these expectations are going

1 to be a first-order challenge. And, two, as with
2 anything, you've got to make sure that the regulatory
3 burden isn't high enough so that only the big
4 companies compete and comply at scale. And so however
5 you design thinking about what expectations are, the
6 expectations of, you know, you have to make sure that
7 startups and large established companies can still
8 compete.

9 MS. CRANOR: Yeah, I actually don't think
10 that makes a whole lot of sense. I think that it's
11 too difficult, as we've discussed here, too difficult
12 to know exactly what the expectations are and what
13 exactly that even means. I think that there are some
14 principles that I'd like to see in a law. I think we
15 want to not surprise consumers, which means we have to
16 communicate with them about what's going on so that
17 they understand what's happening. And I think we
18 should give them choices about the secondary uses of
19 their data. I think that's a much better framing than
20 to say we're just going to meet their expectations.

21 MS. PIRRI: Yeah, I think when reframing
22 expectations as both transparency and control that
23 that is a positive way to address a lot of the varying
24 expectations that we've discussed here on the panel.

25 MR. GILMAN: So we have many more questions,

1 but with three minutes left and people have far more
2 of interest to say than I do, may I just ask if we can
3 go down the line and confine yourself to 30 seconds --
4 there's a clock right there -- in this space that
5 we've talked about today, is there a point we're
6 missing, a question we're failing to ask, or something
7 you'd like to leave us with? Just -- we'll just start
8 at the end, Heather.

9 MS. WEST: Okay. I think that we've touched
10 on this a little bit, but I want to just say it
11 explicitly. People are complicated, and the idea that
12 I am worried about a service but also find it very
13 useful isn't a paradox. They can be both a hundred
14 percent true at the same time. And so as we reframe
15 the way that we think about privacy preferences, not
16 to say that those binary choices aren't important to
17 look at but looking at, you know, integrating that
18 into the context of how we understand, how to build
19 the internet and the technology sector and all of
20 these products and services that we know and love, but
21 we can do it better.

22 MR. GILMAN: Laura?

23 MS. PIRRI: I mean, you know, I think to
24 follow up on that, the US approach has very much
25 historically always looked at balancing considerations

1 around protecting consumers as well as enabling the
2 benefits of innovation. And so, you know, I think
3 that in order to continue that sensible tradition that
4 looking at ways that technology can put the user in
5 the driver's seat is incredibly important as we sort
6 of evolve our privacy policy and approaches.

7 MR. GILMAN: Thanks.

8 Jason?

9 MR. KINT: I would just add from the
10 publisher sector that there's an urgency to this and
11 that there is unfortunately a first-mover kind of
12 disadvantage right now that any -- in the advertising
13 sector, anybody who tries to lead with privacy in
14 meeting consumer expectations actually just gets hit
15 negatively with revenue.

16 And so there is enormous power that is
17 moving towards and has moved over the last 10 years to
18 a very few number of companies for much of the
19 advertising sector. And that is squeezing the oxygen
20 out of the companies that are actually creating the
21 news and entertainment that have historically been
22 responsible for the trust of the public. And it's
23 having societal implications now. That's why we're
24 here and talking about it. And so we need to raise
25 the bar quickly and smartly across the industry.

1 MR. GILMAN: Thanks, Jason.

2 Ariel.

3 Ms. JOHNSON: Just to reiterate that it's
4 critical that everyone thinks about children and teens
5 when designing services. They're probably using
6 yours, even if you are, quote, a general audience site
7 or service, and they both require special protections
8 for different reasons in terms of understanding
9 privacy and understanding how to protect themselves.

10 MR. GILMAN: Great.

11 Avi?

12 MR. GOLDFARB: So at a high level, given the
13 usefulness of data at the same time as consumers'
14 concerns about privacy, I think there's a big question
15 on where is market failure here. We've heard
16 hypotheses around it's about dominance or it's about
17 obfuscation that you're not getting the information.
18 An alternative possibility is that, you know, often
19 the market is working. And so thinking through where
20 the real market failure is sort of core to any
21 regulation.

22 MR. GILMAN: Great.

23 And Lorrie.

24 MS. CRANOR: I think we have to make it
25 really easy for consumers to be able to understand

1 what's going on and exercise their choices. And, you
2 know, the set-and-forget approach is a nice, easy
3 approach, and I know it gets a lot of resistance, but
4 I think we need to find ways of meeting consumer
5 expectations by making it easy for them and to collect
6 data to actually validate that these things work.

7 MS. VANDRUFF: All right. Well, please
8 join Dan and me in thanking our panel for their
9 contributions there afternoon.

10 (Applause.)

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 CURRENT APPROACHES TO PRIVACY, PART 1

2 MS. VANDRUFF: Well, good afternoon, and
3 thank you for joining us. We are continuing our
4 session this afternoon with our panel on the current
5 approaches to privacy. I'm Laura Vandruff. I'm an
6 attorney in the Division of Privacy and Identity
7 Protection, and I'm joined by my colleague, Jared Ho.

8 And let me introduce very briefly our
9 panelists. Their full and impressive biographies are
10 in your materials, as well as online. But very
11 quickly, to my left is Margot Kaminski, and I'm
12 excited that she has a short presentation for us after
13 I quickly introduce the balance of our panel.

14 To Margot's left is Fred Cate. I'm sorry,
15 and Margot, excuse me, Margot -- is an Associate
16 Professor at the University of Colorado Law School and
17 she's the Director of the Privacy Initiative at the
18 Silicon Flatirons.

19 Again, to Margot's left is Fred Cate, who is
20 the Vice President for Research and a distinguished
21 Professor of Law at Indiana University. To Fred's
22 left is Markus Heyder, who is the Vice President and
23 Senior Policy Counselor at Hunton -- excuse me, always
24 Hunton & Williams to me, but it's Hunton Andrews Kurth
25 at Center for Information Policy Leadership.

1 To Markus' left is David LeDuc, and he is
2 the Vice President of Public Policy for the Network
3 Advertising Initiative. To David's left is Laura Moy.
4 She's the Executive Director of Georgetown Law's
5 Center on Privacy and Technology. And finally to
6 Laura's left is Shaundra Watson, Senior Director of
7 Policy at BSA, the Software Alliance, where she
8 provides counsel and develop's global policy.

9 So without further ado, let me introduce
10 Margot Kaminski, who is going to provide a brief
11 overview comparing privacy laws.

12 MS. KAMINSKI: Okay, thank you.

13 MS. VANDRUFF: Thank you, Margot.

14 MS. KAMINSKI: So I have the great pleasure
15 of introducing a number of privacy experts to
16 comparative privacy law, which I hope will not be
17 redundant with what you already know but maybe provide
18 a little bit more of a theoretical framework for how
19 to think about comparisons between US law, European
20 data protection law, and currently proposed state
21 approaches which you've heard about throughout the
22 day.

23 So I'm going to start with an overview of
24 the US federal laws. I'm going to then go to the
25 General Data Protection Regulation, the EU's data

1 protection law, and then I'll talk very briefly about
2 proposed and recently enacted state laws, and all of
3 this in five to ten minutes. Thank you for the
4 laughter.

5 So the basic framework for comparisons here
6 I've gotten from University of Minnesota Professor
7 Bill McGeeveran. And he describes the framework of
8 types of data privacy laws on a spectrum from consumer
9 protection to data protection with hybrid models in
10 between. The consumer protection model, which we're
11 all very familiar with sitting here at an FTC hearing,
12 is the idea of regulating the relationship between a
13 consumer and the business to whom they give their
14 data. This focuses largely on the direct
15 representations of the business to consumer and direct
16 rights that the consumer has with regard to that
17 particular business. What it does less well, as you
18 all know, is reach the behavior of third parties like
19 data brokers.

20 A data protection model, by contrast,
21 follows the data. So there are a series of individual
22 rights, which I'll get into in greater depth shortly,
23 and company obligations, which track the personal data
24 itself rather than focusing directly only on the
25 relationship between the consumer and the business.

1 And many models out there, even within the
2 United States, are hybrid models somewhere between the
3 point of the spectrum.

4 So additional points of comparison you'll
5 hear in my remaining eight minutes. One, obviously
6 there's a difference between omnibus data protection
7 law and sectoral data protection law or data privacy
8 law -- data privacy law that focuses on a particular
9 sector, particular type of business or particular type
10 of information versus data privacy law that is
11 supposed to follow all kinds of personal data in all
12 sectors.

13 We have the contrast between a notice and
14 choice model, which often is employed at some way in
15 the consumer protection model and sometimes within a
16 data protection model as well versus sort of
17 augmentations to notice and choice that focus more on,
18 for example, company obligations or duties, even in
19 the absence of individual invocation of rights. And
20 that goes to a contrast between an individual rights
21 regime that gives individuals notice rights, access
22 rights, control over data versus a compliance regime
23 that focuses more on appointing data protection
24 officers or having data protection impact assessments
25 and not just the duties that companies owe to

1 individuals but the management and risk assessment
2 regimes for data running through their companies.

3 There is a contrast -- this is much higher
4 level -- but between hard law and soft law, both rules
5 versus standards in different kinds of compliance. So
6 you can write a law that is extremely specific ex ante
7 in its requirements or a law more like the GDPR that
8 is extremely vague ex ante in its requirements and
9 gets constituted through back-and-forth between
10 companies and the regulators.

11 So I'm starting with current federal law,
12 the first of which I should be able to spend just a
13 very short amount of time with. The Federal Trade
14 Commission, again very familiar to all of you here, is
15 largely in McGeveran's scheme a consumer protection
16 model. It is omnibus-ish in the sense that there are
17 clear exceptions from it, including for nonprofits,
18 including gaps in coverage of third parties, but
19 compared to US sectoral laws, including some that the
20 FTC enforces, it's more omnibus than other regimes.

21 Then we have our federal sectoral statutes,
22 again which I'm sure we'll talk about at greater
23 length during this panel -- HIPAA, COPPA, the Gramm-
24 Leach-Bliley Act, all of which target either specific
25 entities or specific types of information or

1 combinations of both. These have data protection-like
2 features. So sometimes there are rules that follow
3 the data as opposed to rules that just focus on the
4 direct relationship between a consumer and a company.
5 But they're not data protection-like in the
6 comprehensive way that, say, the GDPR is.

7 And they largely still, even within that
8 data protection-like framework, do focus heavily as a
9 matter of historic accident, if not policy choice, on
10 the idea of individual notice and choice. So even in
11 a data protection framework, they're more on the
12 notice and choice than on the compliance governance
13 side of that regime. And we can debate that later if
14 needed.

15 The GDPR -- wow, that's small font -- the
16 GDPR, on a very high level, differs in a number of
17 ways from US regimes, as you all know. First, it is
18 absolute an omnibus type of regulation. I'm going to
19 largely talk about it as it applies to companies
20 because that's the impact for individuals in the
21 United States or companies in the United States, but
22 it's omnibus in the sense that it follows all personal
23 data and all processing of personal data with
24 exceptions for personal household use for the context
25 of criminal law and the context of national security,

1 among other things.

2 The definition of personal data is extremely
3 broad, rivaled probably only by the definition of
4 personal data in the California Consumer Protection
5 Act. The GDPR represents the data protection model
6 par excellence, right? The laws follow the data.
7 They very clearly apply to third parties that hold
8 data they did not obtain originally from an individual
9 with whom they had a consumer relationship. And that
10 includes especially coverage of third parties. In
11 fact, arguably, the GDPR puts more onerous
12 requirements on third-party data brokers than it does
13 even on the companies that have direct business
14 relationships with consumers.

15 It's hard law along some lines. There are,
16 again, famously significant fines that attach if
17 regulators decide to use them in enforcement, and
18 there are both individual rights of enforcement,
19 regulatory enforcement, and serious court involvement.
20 And this is combined -- this system of hard law is
21 combined in the GDPR with softer law which ranges from
22 just the inclusion of broad standards that will
23 eventually get fleshed out through back-and-forth
24 between companies and regulators. And in addition to
25 those broad standards, specific formal mechanisms of

1 collaborative governance contemplated, like, codes of
2 conduct or certification mechanisms.

3 So the core elements of what's in the GDPR,
4 and here I'll go a little bit faster, we have a system
5 of individual rights. This is what most US persons
6 think of when they think of the GDPR. They think of
7 the rights of notice, the subject access rights, the
8 right to deletion, famously, you know, described as
9 the right to be forgotten.

10 And on the other side, less notice by US
11 persons usually or the obligations for companies but
12 very noticed obviously by companies. The individual
13 rights are FIPPs-like. They are Fair Information
14 Practice Principles-like. They include notice rights,
15 access rights, a correction right, erasure, famously
16 data portability, also famously a right to contest
17 algorithmic -- solely automated algorithmic decisions.

18 And then the obligations for companies,
19 which form what I would argue is the bulk of the
20 GDPR's impact, stem from this idea, this core
21 principle from the GDPR of accountability. So this is
22 the idea that companies not only need to institute
23 complex, internal compliance regimes, but they need to
24 be accountable throughout internally and, if
25 regulators choose to ask for it, and for some

1 mandatory reporting requirements directly to the
2 regulators.

3 So this means that companies looking at the
4 GDPR have to be thinking very strategically and in-
5 depth about not just filling the checklist of
6 compliance but being able to demonstrate their
7 compliance with the GDPR. The second element of the
8 GDPR that is really notable, especially when
9 contrasted with US laws, is this core principle of
10 lawfulness, so processing must be lawful. This is not
11 something that you really see in even US data
12 protection-like laws.

13 When a data controller, meaning the company
14 that determines the means, purposes, et cetera, of
15 processing of data, processes personal data, it has to
16 have a legitimate ground for processing, and a number
17 of US persons looking at the GDPR in passing may
18 confuse this with a notice and choice regime and think
19 that legitimate grounds for processing just means you
20 have to get somebody's consent.

21 In practice, as many of you know, again,
22 companies often avoid consent because consent can be
23 withdrawn under the GDPR and instead choose other
24 legitimate grounds for processing. Obligations also
25 include all of the above, transparency requirements;

1 affirmative notice requirements, not just when
2 individuals ask for access, but affirmatively to
3 individuals who haven't yet asked; documentation
4 recording requirements; security obligations; the
5 requirement in some circumstances, high-risk
6 circumstances, that you appoint a data protection
7 officer; conduct impact assessments; and the
8 famous/infamous requirement of data protection by
9 design and by default, which again is largely a
10 designing corporate governance -- internal corporate
11 governance mechanism type of requirement.

12 So, overview summary of the GDPR, the GDPR
13 is a hard law data protection regime in that it's
14 backed by significant enforcement capabilities and
15 multiple prongs of enforcement, not just from
16 regulators but also by individuals, but it has
17 significant soft law and collaborative features within
18 it. And these requirements focus on both individual
19 rights and significantly possibly more significantly
20 worldwide company compliance.

21 All right. So in my remaining few seconds,
22 by comparison, the California Consumer Privacy Act,
23 which you've heard about a lot throughout the day, it
24 is somewhere between consumer protection and data
25 protection. So there are elements of it that focus

1 primarily on the relationship between a consumer and
2 the business that gathers consumer data directly from
3 the consumer. And there are other elements of it that
4 do actually follow the data, which is different from
5 most US existing privacy regimes.

6 It's omnibus but it's only omnibus-ish in
7 that it focuses on businesses with the definition of
8 "business" being a subset of three different kinds of
9 businesses. The definition of personal information,
10 however, is broad, extremely broad, and possibly
11 arguably broader than the definitions within the GDPR.

12 The California Consumer Protection Act
13 contains notice and access rights, which are similar
14 to the GDPR but in their granular details differ in
15 ways that could raise regulatory costs for companies.
16 It has a limited deletion right -- emphasis on limited
17 -- in that the deletion right attaches more to the
18 consumer protection relationship or consumer
19 protection review of privacy than to third parties.

20 It has a limited opt-out right, again, of
21 sale of data, but not in other contexts. And its
22 enforcement mechanisms are very different from the
23 GDPR. There's no individual right of action. It's
24 enforceable largely by the state attorney general,
25 except in a specific data security context, and that

1 state attorney general is also the regulator
2 responsible for promulgating rules that clarify some
3 of the obligations under the law.

4 So, in short, they overlap pretty
5 significantly, the CCPA and the GDPR, when you're
6 talking about the parts that deal with transparency
7 and individual control, the aspects of data protection
8 that look most like, say, open government laws in the
9 United States. But they diverge really significantly
10 on what I've called the most important part of the
11 GDPR, which is the compliance or company obligations.

12 There's nothing in the CCPA that includes
13 anything on legal basis of processing. There's
14 somewhat a light purpose specification requirement in
15 the disclosure requirements. There's no use
16 limitation. There's no data minimization. There's no
17 DPO requirement. There's no DPIA requirement, et
18 cetera. And they have vastly different enforcement
19 mechanisms with a private right of action in the GDPR
20 that allows individuals in Europe to invoke the pro-
21 data-protection inclinations of European courts. And
22 they have vastly different court contexts to that
23 point exactly.

24 Okay. So, I'll close here. The proposed
25 state laws that we've seen around the country, and

1 we've seen probably almost all of the states impose
2 something that they call or propose something that
3 they call data privacy laws in the last year. They
4 largely, to the extent that they are data privacy and
5 not just data security under the guise or name of data
6 privacy, as my home state of Colorado has, to the
7 extent that they are data privacy laws, they're
8 largely directly mimicking the CCPA and not mimicking
9 the GDPR.

10 They evidence, nonetheless, a significant
11 paradigm shift in US data privacy laws because there's
12 this shift from the sectoral mode to the omnibus,
13 again, omnibus-ish mode. And there's a shift towards
14 data protection of protections that follow the data
15 away from just the consumer protection model that
16 we're used to in this context.

17 Various variations, we've seen some of the
18 proposed laws, not enacted yet, but some of the
19 proposed laws add a private right of action. Some
20 establish exploratory committees rather than actually
21 establishing law. And many focus on data security,
22 even though they are proposed under the moniker of
23 data protection or data privacy.

24 So, with that, I will turn it over to my
25 fellow panelists. Thank you very much for your time.

1 MS. VANDRUFF: Okay. So, that was
2 tremendous. I learned everything I needed to know.
3 No, in all seriousness, that was a very quick
4 overview, but really very substantive. But I wanted
5 to just open it to the panel at the outset to see if
6 anyone had any high-level comments on the differences
7 and approach that you see between the GDPR, CCPA, and
8 the US sectoral-specific approach in self-regulation.

9 And if not, then I can move on to a
10 different question.

11 MS. MOY: I mean, I think that -- so, Margot
12 did a great job. Thank you so much for that summary,
13 Margot. That was fantastic and really helpful.
14 Margot did a pretty good job highlighting some of the
15 high-level differences of them. The sort of vast
16 comprehensiveness of GDPR, the much more limited in
17 scope nature of CCPA, and, of course, the sectoral
18 laws.

19 I think I would highlight a couple
20 differences. So, one is the enforcement of GDPR. So
21 something that GDPR does that is kind of new and
22 probably -- likely will make a big difference in
23 seeing the impact that this law has is that it allows
24 for fines of up to 4 percent of a company's annual
25 revenue for violations of GDPR. And those are

1 potentially tremendous fines, right? I mean, if you
2 look at some of the biggest fines that we've seen in
3 the US under Section 5, you're looking at fines that
4 could amount to hours rather than days or weeks of a
5 very large company's revenue for violations of consent
6 decrees that have been agreed upon under Section 5.

7 But, you know, a 4 percent fine -- 4
8 percent of annual revenue is much bigger, and the idea
9 there -- the thinking there is that a higher fine
10 makes privacy into something that rises from the level
11 of something that's just a cost of doing business to
12 something that becomes a boardroom-level conversation,
13 because the cost of violation is so tremendous. So
14 that's just one big difference that I would highlight.

15 MS. VANDRUFF: Markus.

16 MR. HEYDER: Yes, thank you. So the one
17 thing that I want to highlight that's a big difference
18 between the GDPR and the CCPA, for example, is that
19 the CCP -- the GDPR provides for a comprehensive
20 approach to privacy, and the key element to that, I
21 think, is the fact that it codified the concept of
22 organizational accountability, which essentially
23 focuses and forces organizations to develop
24 comprehensive privacy infrastructures that cover the
25 entire data cycle throughout the data lifecycle,

1 throughout collection up until use and disposition of
2 the data.

3 And it really provides a framework for
4 moving away from the individual control model, the
5 notice, choice, and consent model, in that it entails
6 many other data and privacy-protective tools that are
7 part of the concept of organizational accountability.
8 So I think this is an important difference between the
9 GDPR and the very narrow CCPA. And I think when we
10 talk about what a US privacy framework should look
11 like, we should look at the concept of organizational
12 accountability and take that and implement it in the
13 US as the foundation for a comprehensive approach in
14 the United States.

15 We can talk about organizational
16 accountability more, but key elements are formal
17 accountability schemes like certifications and codes
18 of conduct, which is what Margot already pointed out
19 that they are an element of the GDPR. That's also --
20 we think that's also going to be a very important
21 component for US privacy legislation in the future to
22 enable third-party involvement through formal schemes
23 like codes and certifications to free up privacy
24 enforcement authorities like the FTC to focus on
25 what's important and to extend and augment the reach

1 of privacy enforcement through these third-party
2 privacy accountability schemes like certifications and
3 codes of conducts.

4 And one example that we like to point out --
5 point to are the APEC cross-border privacy rules,
6 which we think should be part of any US framework
7 going forward. And the other important element is
8 that the entire GDPR's underpinned by a risk-based
9 approach to privacy that means that all data-
10 processing activities have to be subjected to a risk
11 assessment of some sort.

12 In some contexts, risk assessments have to
13 be at a higher level and require full-blown data
14 protection impact assessments, but the general idea of
15 understanding a processing in terms of risks and then
16 devising mitigations and controls specifically
17 targeted to those risks is very important and is the
18 other key element I think we can learn from the GDPR
19 for a US framework going forward. There are a lot of
20 issues, but these are the two key distinguishing
21 factors that I can point to that I think are
22 important.

23 MS. WATSON: And I just wanted to pick up on
24 I think something that both Markus and Margot
25 mentioned with respect to the accountability piece.

1 We hear a lot about in discussion of what a new
2 federal law should look like. You know, are you going
3 to replace California? And our response to that
4 question is that, first of all, a federal law doesn't
5 mean it needs to be a weak law, and we want to
6 actually strengthen the protections that are in CCPA.
7 And when we say that, I think we are sort of referring
8 precisely to what Markus is alluding to with respect
9 to accountability and with respect to what Margot said
10 about sort of regulating the first party use of
11 information.

12 And so CCPA doesn't really sort of get at
13 that underlying risk assessment and what first parties
14 are doing to protect data sort of aside from the
15 sharing of data. And that's an area where I think we
16 think it's really useful and that's an area where GDPR
17 is also useful.

18 I think another important difference between
19 the GDPR approach and the approaches that we've seen
20 in the United States is that GDPR is obviously built
21 on an EU model, a civil code model. And so that
22 necessarily means that the provisions are more
23 proscriptive and more detailed. And what we've seen
24 in the US is an approach that strikes a little bit of
25 a different balance and, therefore, you have a little

1 bit more flexibility in how you do things.

2 And so I think we should also highlight as
3 part of this conversation, obviously, there's CCPA,
4 and a lot of states are introducing laws that mimic
5 those protections or adapt them slightly, but there's
6 also a Washington bill pending, and that bill takes a
7 very different approach. And in many ways, it's more
8 comprehensive like GDPR, but I think it sort of makes
9 adaptations that are more reasonable for the US
10 context.

11 And, in particular, there are risk
12 assessments that are described there, but essentially
13 the company is assessing a risk and they're
14 documenting it, but they're not providing that
15 information to the DPA, you know, unless it's upon
16 request, whereas in GDPR, you know, if it meets a
17 certain risk level, you are consulting with the DPA on
18 that processing, and before you can proceed, there's
19 some back and forth. And so I think that may create a
20 little bit of friction in terms of companies providing
21 services.

22 And so, we see different approaches. Like,
23 we share the overall arching aim of GDPR is to provide
24 consumers with more control over their personal
25 information and to ensure that companies are

1 accountable, and we share the same goals. But I think
2 the real question is how do we implement those
3 protections in a meaningful and effective way, in a
4 way that is -- fits the US legal culture and legal
5 context. And so I think we've seen a number of
6 different approaches, but I think those are some
7 differences that I would highlight.

8 MR. LEDUC: And I'd love to jump in, and I
9 guess I'll agree a lot with what Markus said and
10 certainly what Shaundra said as well. With respect to
11 the -- you know, I mean, I think most top of mind for
12 everyone is really CCPA and GDPR. You know, they're
13 the two newest laws, so I think it's fair to kind of
14 hash those out and compare and contrast those.

15 And while I agree with Markus about the GDPR
16 and its structure and I think -- I guess its movement
17 away from notice and consent by design, I think that's
18 absolutely true, but by implementation, unfortunately,
19 it ends up being not the case. You know, and I think
20 because we've got an ambiguous implementation
21 structure, really in enforcement, what we end up with
22 is a regime that is falling back, certainly in the web
23 context, is really falling back to reliance on
24 consent.

25 And I certainly don't think that's the

1 intent of GDPR, I mean, as written, but it's the
2 reality. If you look at CCPA, we've also got a new
3 law that's very focused on notice and control. And,
4 you know, speaking on behalf of NAI and the digital
5 advertising industry, those elements, the FIPPs,
6 they're critical to data responsibility, but at the
7 same time, we really feel like -- you know, Margot
8 used the term "paradigm shift." I mean, we really
9 feel like it's time. We need a paradigm shift back
10 towards accountability as Markus mentioned. We need
11 to have privacy laws that focus more on data uses and
12 harms rather than trying to saddle consumers with the
13 responsibility of having to manage their data.

14 And I think, you know, while that will
15 remain a critical element, you know, notice and
16 control, transparency will remain critical, the notion
17 of going about it as the primary means for privacy
18 protection is just not very effective.

19 And another element I would point out about
20 the CCPA, which I haven't heard come up much today, is
21 that CCPA is very unusual in focusing on just the
22 sale. So it creates this concept, and I think this
23 false sense of security or privacy to consumers, the
24 notion of, well, if your data's not being sold, then
25 it's just fine. You know, if your data's collected by

1 a first party, that's great, you can trust them, but
2 it's the third parties.

3 We heard secondary uses a lot today. The
4 notion that secondary uses of data are inherently bad
5 and wrong and they need to be protected. In some
6 cases, that's certainly true. But in other cases,
7 there are certainly first-party actors that can
8 collect data and misuse that data and not protect that
9 data. So the notion that we need to be protecting
10 consumers on the basis of a sale, a transaction from a
11 first party or third party, I think is inherently
12 flawed.

13 And I think, you know, as many of us are
14 looking at the CCPA, how it will be implemented, I
15 think people are going to be very disappointed with
16 respect to, you know, that as a framework and in terms
17 of -- and so when we talk about -- like Shaundra said,
18 when we talk about a federal law, I mean, I think we
19 can look at the GDPR, we can look at the CCPA, try to
20 take the best elements of those, try to take the
21 flexibility from the GDPR that I think was intended
22 frankly that could be implemented, try to take some of
23 the protection -- the protections, the controls for
24 consumers conceptually from the CCPA, make sure that
25 consumers have those, but really focus on data use, on

1 reasonable uses, focus on those, try to get those out
2 of the system.

3 MR. HO: So I think it's fitting that we
4 started out this morning talking about the goals of
5 privacy protection, and now that we have this panel on
6 the current approaches and have been discussing the
7 specific privacy laws, I think it would be helpful to
8 put some meat on the bones. And so, Laura, maybe
9 would you mind kicking us off on sort of your thoughts
10 on what the harms that these laws that we've been
11 talking about are trying to address? And then we can
12 open it up to the panel for discussion.

13 MS. MOY: Sure. Yeah, I'm happy to do that.
14 And I think, you know, Margot and the rest of the
15 panel have touched a little bit on this, that both the
16 CCPA and GDPR primarily are focused on linkable,
17 tangible harms to the individual and to the
18 transparency and control that an individual may need.
19 So the harm may be lack of transparency, a lack of
20 control to the individual, but really focused
21 primarily on the individual, also thinking about
22 individual rights in the GDPR context.

23 And I think that's something that we're
24 starting to see in some of the conversations around
25 where privacy might go in the US, is we're starting to

1 talk more about harms that are not necessarily
2 linkable and tangible with respect to the individual.
3 And, David, I actually think that your comments are
4 getting there a little bit, thinking about some first-
5 party uses of data, that some of the -- some of the
6 things that we might find most concerning about
7 uncontrolled uses of information, about consumer
8 information right now might be harms like
9 discriminatory advertising, right? They might be
10 harms that fall more broadly on society where it's
11 very difficult to see exactly what the impact is on an
12 individual.

13 So discriminatory advertising, amplification
14 of hate speech, political polarization,
15 misinformation, and disinformation. These are a bunch
16 of the things that we're kind of seeing now at the
17 society level that could be harms stemming from uses
18 of information and that some of these more traditional
19 individual-focused privacy frameworks don't
20 necessarily get it at but where the conversation is
21 starting to go.

22 So, you know, for example, we saw, I think,
23 44 civil rights and privacy organizations, our
24 organization was one of them, send a letter to
25 Congress a couple months ago highlighting the civil

1 rights principles in the era of big data and talking
2 about the importance of protecting civil rights in the
3 area of big data and centering these considerations
4 about societal harms in conversations about privacy.
5 But those really are societal harms that traditionally
6 we haven't seen centered in privacy conversations and
7 maybe haven't seen centered in these laws.

8 I think one exception maybe is -- it
9 actually comes from sectoral laws in the US, where you
10 could think of sectoral laws in the US as being framed
11 around the rights of an individual to protect themselves
12 against harm that may flow from use of particularly
13 sensitive information shared in a sensitive context.

14 But another way to look at sectoral laws is
15 as a way of protecting, or I should say encouraging,
16 relationships between individuals and companies or
17 providers in contexts where we view information
18 sharing as essential or where we view services as
19 essential. So we have these sectoral privacy laws in
20 context like healthcare, education, finance, where we
21 really want to create trust and incentives for our
22 consumers to share information.

23 And that really is sort of -- those sort of
24 are interests viewed through a societal lens and less
25 through a private -- through an individual lens. So,

1 again, I think that largely we've seen these laws
2 focus on the individual, but we're starting to see the
3 conversation shift more toward privacy interests that
4 affect society.

5 MR. CATE: Can I just say it was a leap, a
6 welcome leap, to my mind, so I'm very complimentary
7 that, Jared, you started with goals and then you said
8 harms. And for two-thirds of the world, they would
9 not agree that harms are the goals of data protection
10 laws. I mean, GDPR certainly doesn't believe that.
11 And, frankly, up until quite recently, the US didn't
12 believe it. I mean, we've been saying it. The
13 Supreme Court has been saying it. The Federal Trade
14 Commission said for over a decade that the goal of
15 privacy protection is consumer control of information,
16 and, therefore, any uncontrolled use was itself
17 violating that principle.

18 This is, of course, meaningless today when
19 almost all use of information occurs outside of
20 individual control. Nor would we want to try to
21 control it. I mean, think about a world of internet
22 of things and artificial intelligence and big data,
23 and it's a little bit silly to think that an
24 individual is going to exercise control or really
25 wants to.

1 What we want is for our information to be in
2 control, to be subject to some sort of type of
3 protection that will assure us that, if we are harmed
4 by it -- and so, in fact, moving the discussion out of
5 Europe, out of CCPA to instead say, let's talk about
6 what are the actual objectives, what are the harms we
7 are trying to avoid. Those harms may be physical.
8 They may be financial. They may be emotional. I
9 mean, we recognize emotional harm in other areas of
10 tort law. There's no reason we wouldn't recognize
11 them here. But that use without control by itself is
12 not going to be a harm.

13 And this is in many ways the great challenge
14 of the GDPR. There are a lot of great things in it,
15 but there should be because everything is in the GDPR.
16 There's nothing left out.

17 (Laughter.)

18 MR. CATE: It's got accountability. It's
19 got risk management. It's got FIPPs. It's got
20 consent use 72 times in it, and as a result, you can
21 find anything you want in the GDPR and have no idea
22 what your objective is in trying to comply with it.
23 That's why regulators in Europe are having so much
24 trouble coming up with common standards for what to
25 use. That's why companies are spending billions of

1 dollars on lawyers, which I think is a great thing,
2 and I encourage you to do more of that.

3 (Laughter.)

4 MR. CATE: But that's not a successful
5 privacy law if you bring everyone in a room and nobody
6 agrees what its purpose is. So starting with goals is
7 a really great thing to do, and if those goals are
8 avoiding harms, then defining those harms is a great
9 place to start and would be really useful in the
10 regulatory or legislative environment in the United
11 States.

12 MR. HO: Markus.

13 MR. HEYDER: Thanks, Jared. And I wanted to
14 go in the same direction as Fred just went. I just
15 want to make one additional point is that when we
16 start out, I think the first question around goals
17 should be the bigger issue is that there really are
18 two goals or there ought to be two goals. One is to
19 protect individuals against harm; the other goal of a
20 privacy framework should be to enable the beneficial
21 use of information.

22 Since data privacy laws, data protection
23 laws deal with the handling and use of data, it has to
24 -- everything has to be looked at through the lens of
25 how can we use data beneficially in a way that it

1 doesn't hurt consumers? So these are actually two
2 separate goals that always have to be kept in mind,
3 and they should be explicitly stated in a privacy law.
4 I believe the Brazilian privacy law actually says that
5 right up front. There are two goals to privacy laws,
6 protect privacy and enable the use of information.

7 And the whole issue of secondary uses and
8 how we handle them and how we take the consumer out of
9 making daily decisions about how data is being used,
10 secondary uses and so on and so forth, goes to that
11 issue.

12 MS. KAMINSKI: So I want to keep this
13 relatively brief because I had the privilege of
14 speaking at the beginning of this panel. But the
15 question of harm, I agree with Fred that the notion of
16 harm alone doesn't get you what data protection
17 regimes are doing and that articulating goals aside
18 from the articulation of harm is also important.

19 I wanted to bring us back a little bit to
20 what Laura said about the prospect of collective
21 harms, because this is definitely one of the stronger
22 criticisms of the GDPR as a regime that by focusing so
23 squarely on the individual, it leaves out the kinds of
24 harms that we see on a more society-wide level.

25 That said, the compliance or governance

1 aspects of the GDPR which require risk assessments, as
2 Markus mentioned and I discussed in the opening
3 presentation, those do encourage, at least if not
4 require, companies to think about things on a broader
5 impact level. And that's the part of the GDPR that is
6 most of interest to me because it moves away from this
7 notice and choice -- solely notice and choice regime
8 to starting to think about the impact of data use more
9 broadly on society as a whole.

10 The second prong I wanted to introduce into
11 this is that we're all having this conversation in the
12 United States where the notion of data privacy harm is
13 highly contentious in comparison to Europe where it's
14 barely questioned. And you see this in particular
15 with the individual causes of action on the GDPR where
16 an individual just de facto has standing to bring
17 these claims.

18 In the US -- and this was a big issue in the
19 invalidation of the safe harbor mechanism and remains
20 an issue in the conversation about the Privacy Shield
21 as mechanisms for transferring data from the EU to the
22 United States. The question whether individuals can
23 can have standing even under our existing sectoral
24 privacy laws is hotly contested. And I think just as
25 a broad-level observation, you see this strange

1 parallel of two minds set of jurisprudence arising at
2 the Supreme Court where the standing doctrine on the
3 one hand arguably seems to be moving towards really
4 concrete, Scalia-style ideas of harm as measurable in
5 terms of money, reputation, et cetera, where the
6 Fourth Amendment jurisprudence of the United States
7 increasingly looks at what we consider to be more big
8 data or mosaic-theory-based and understandings of harm
9 where you see in Carpenter, for example, or in Jones
10 society-wide assessments of the possibility of a
11 chilling effect from data misuse or from extreme
12 collection, even in public spaces. And it seems to me
13 that the Supreme Court has not yet put together those
14 two prongs of jurisprudence to try to figure out how
15 they interact with each other along the issues of what
16 privacy harm actually is.

17 MS. VANDRUFF: Well, Margot, you've raised a
18 number of really interesting issues, many of which
19 touch on the question that I wanted to ask next, which
20 is what mechanisms different privacy models, including
21 the ones that you introduced to our audience, what
22 mechanisms they have to incentivize firms to protect
23 consumer privacy?

24 And Markus raised the question of protecting
25 the individual versus enabling the use of information.

1 So query what privacy even means, but what mechanisms
2 different models have to incentivize protecting
3 consumer privacy. So, for example, are civil
4 penalties a deterrent? That is an example of one
5 mechanism, but there are myriad of others, and so I
6 invite the panel to address that.

7 Yes, Shaundra.

8 MS. WATSON: Yeah, I think civil penalties
9 are absolutely a deterrent. You've seen it with the 4
10 percent of global turnover for GDPR fines. And that
11 definitely got the attention of the C-suite level of
12 the board, which was good in a way because it provides
13 privacy professionals with the funding and the
14 internal support to implement the protections that
15 they need to implement. And with respect to the
16 conversation about a US federal law, my organization,
17 BSA, supports the ability of the FTC to get new
18 authority for initial violations of Section 5.

19 So we think that civil penalties play an
20 important role and we support that. But I think it's
21 important to remember that civil penalties are sort of
22 not the only part of the story. And I think it's
23 important to ask the question about sort of what else
24 can you do to provide flexibility within the law that
25 would incentivize companies to provide meaningful

1 privacy protections.

2 And one example, I think, alludes to
3 something that I think that was discussed on the de-
4 identification panel earlier this morning. And so
5 when we talk about de-identification in the context of
6 GDPR, the European Data Protection Board's predecessor
7 looked at this issue and essentially requires
8 anonymization. And so within the GDPR, you're not
9 exempt from requirements because you're taking steps
10 to de-identify data. It's a mechanism to help you
11 achieve compliance but the requirements are not
12 otherwise relaxed.

13 And so, I think this is an area that could
14 actually incentivize companies. So will companies
15 really spend the money to invest in the research for
16 differential privacy and other privacy-enhancing
17 technologies if they're not going to get some sort of
18 corresponding benefit in the law? And so, I think
19 incorporating that type of flexibility within the law
20 would also incentivize companies to implement
21 additional protections.

22 MS. VANDRUFF: Markus?

23 MR. HEYDER: So, in addition to fines, as
24 Shaundra mentioned and the other items she mentioned,
25 I would, again, point to the concept of organizational

1 accountability, which requires organizations to
2 implement comprehensive privacy management programs,
3 which is essentially an ex ante exercise to prevent
4 bad outcomes at some point and to avoid ex post
5 enforcement. So that's a huge ex ante mechanism to
6 get companies up to speed in terms of protecting
7 privacy.

8 And if in addition to that they use formal
9 accountability schemes like GDPR certifications or in
10 the US some other form of certification, maybe APEC
11 CBPR or industry codes of conduct or something like
12 that, that again provides for engagement with the
13 third-party accountability agent or certifying body,
14 all ex ante efforts, you know, back-and-forth dialogue
15 in terms of getting companies into compliance with
16 that code or certification. That's a huge -- this
17 concept of accountability, formal or informal, has
18 huge potential for ex ante efforts to avoid bad
19 outcomes in the end.

20 And, finally, also from the GDPR, we can
21 take the concept of data protection officer, or the
22 DPO, which certain organizations have to have if they
23 meet certain criteria, which also forces organizations
24 to focus on privacy right from the start and to have
25 somebody in charge and responsible and accountable for

1 implementing a comprehensive privacy management
2 program.

3 MS. VANDRUFF: Margot?

4 MS. KAMINSKI: So yes. So the GDPR
5 aspirationally is largely a collaborative governance
6 regime where what regulators are looking to do in --
7 for the most part leaving aside individual rights for
8 a second, apologies to all Europeans in the room, but
9 what regulators are trying to do is to get private-
10 public partnerships in filling out these broad-level
11 standards so you have a very vague standard in the
12 text and then you have encouragement of private
13 companies to come in and say, well, this is how we're
14 going to implement it in our sector and in our
15 practices.

16 For that to work, for that kind of private-
17 public partnership to work, you have to have
18 regulators who are both capable of issuing big sticks
19 and decent carrots. So the regulator has to, as Laura
20 pointed out, have enough of a capability of issuing
21 fines or invoking some other form of penalty that
22 companies are incentivized to actually get in the
23 room, but at the same time, they need to be able to
24 sort of hold off on those fines if necessary to make
25 the companies feel like this is a safe space for

1 disclosure, and that balance is incredibly notoriously
2 hard to strike.

3 On the one side, it can end up going in the
4 direction of capture where the agency ends up being
5 bedfellows with the company. Or, on the other side of
6 things, it can end up being that you have such an
7 enforcement-prone agency that companies don't see the
8 incentive to get in the room and provide the details,
9 and then it just becomes vague standards that nobody
10 can comply with. I think that the component of the
11 GDPR that is hardest to replicate in the United States
12 is the courts.

13 So even if we end up putting in place a
14 system of individual rights, we still don't have
15 either CJU case law or European fundamental rights
16 documents that put data protection or privacy on equal
17 footing with the First Amendment, and that makes
18 calibrating this space for collaborative governance
19 extremely tricky in the United States, because there,
20 even if you put in place a large fine or significant
21 penalties, you run the risk that courts are going to
22 end up undermining that in light of really significant
23 important First Amendment values or First Amendment
24 doctrine.

25 MR. LEDUC: I mean, I think that really

1 underscores your point about this delicate balance but
2 a critical balance between regulation and kind of co-
3 regulation, right? I mean, we talked about that, and
4 it is hard to do, but we do have precedent for that
5 here in the US, and I think it's a very, very strong
6 model going forward, I mean, the notion that we would
7 have a comprehensive federal privacy law and have it
8 be able to be enforced without some element of co-
9 regulation where we have public-private partnership
10 and the ability to help.

11 I mean, we also agree that the FTC should
12 have expanded authority. We agree in the ability to
13 have civil penalties. We agree with enforcement by
14 state attorney generals. But at the same time, we
15 still think it's critical, particularly in a world of
16 the IOT and just a tremendous amount of data
17 collection and use. Without some element of co-
18 regulation, it just can't be effectively done.

19 We can't have this worked out through the
20 courts. We certainly don't want it done through a
21 private right of action where, you know, we're just
22 litigating it. That's not the model. We do have a
23 model. And I think, you know, there have been
24 concerns raised, frankly, about COPPA, which is, you
25 know, one of the best models that we have. And I

1 think some of those are fair concerns, frankly.

2 You know, but we have the ability to, I
3 think, empower the FTC to -- and have a federal law
4 establish tighter rules around organizations that can
5 then provide rules for companies to follow. And,
6 again, I mean, we can't lose sight of -- and I think
7 Markus said this very well -- the notion of the goals
8 here, wanting to balance the privacy protections,
9 prevent the harmful uses of data but allow for the
10 innovation.

11 When you're doing that, I mean, we really
12 need to have a structure that's flexible enough to
13 provide for that and to make that balance.

14 MR. CATE: Let me just jump in one second.
15 I think there are two things we have to keep in mind,
16 though. And one is big fines with ambiguity in the
17 law are a disaster, and they have almost no incentive
18 effect. So, yes, they get everyone's attention, but
19 everyone's sitting around scratching their heads,
20 saying I have no idea what to do next because look at
21 them, what they just paid and they did X, Y, and Z and
22 got no credit for it.

23 On the other hand, always a penalty is a
24 failure. In other words, it means, the privacy has
25 been violated, the harm's been done, and now we've got

1 a penalty. So, really coming back to Markus' point,
2 the more we can do that tries to avoid that, that
3 tries to create incentives for the better behavior up
4 front, whether that's safe harbors for certain types
5 of behavior, whether that's encouraging, you know,
6 data review boards or other types of accountability
7 tools, that the goal is to avoid the situation where
8 we're saying we got you for having done it wrong.
9 What we want to do is have it not go wrong in the
10 first place.

11 MS. MOY: Yeah, I agree with that. And I
12 think that that's one of the reasons that rulemaking
13 can be a really important tool, right, to create some
14 certainty at the outset as to what the specific rules
15 are as opposed to the general rules. I also wanted to
16 just amplify the mention just a moment ago, I think,
17 by David, of the role of state attorneys general,
18 because I think, you know, having more cops on the
19 beat to potentially -- not only to enforce but to help
20 those who are attempting to comply with the law to
21 understand what the law is, provide guidance, right,
22 is something that can help to encourage compliance.

23 And the CCPA does this a little bit. CCPA
24 does kind of create actually the requirements, I think
25 -- someone correct me if I'm wrong here -- that the

1 state AG provide opinions to companies that are
2 seeking opinions. Of course, one of the big problems
3 is that it creates a bit of -- it creates in this
4 instance a bit of a conflict sometimes for that agency
5 and also I think creates this new obligation without
6 establishing additional resources for the state AG's
7 office to carry out those responsibilities. But there
8 is a recognition that there's a role to play here for
9 an entity to help translate the rules for companies
10 that are trying to comply.

11 I mean, the FTC is doing a lot on privacy
12 but -- and correct me if I'm wrong on this -- I think
13 that it's an agency with about 1,100 staff to it, and
14 that that agency does a lot more than just try to
15 protect consumer digital privacy. So, we need more
16 cops on the beat, more agencies, ideally state AGs as
17 well to help with compliance.

18 MS. KAMINSKI: Just one quick wrap-up, and
19 apologies to Fred for having interrupted earlier. So,
20 this idea that broad standards plus heavy fines is a
21 recipe for corporate compliance disaster I do think
22 runs really counter to how this is thought about in
23 the EU. And not to pick sides on which form is right,
24 but to the extent that we're moving towards a federal
25 privacy law that potentially preempts state privacy

1 laws, it's almost inevitable that we're going to be
2 moving to a vaguer standard as opposed to precise
3 rules in that context.

4 And so this -- we're facing a fork in the
5 road basically on which version of this we want to end
6 up doing, and I would just suggest that rushing to a
7 federal privacy law that does preempt state ability to
8 experiment in this area does suggest a push towards
9 broader standards as opposed to more specific rules.

10 The second thing I wanted to bring up just
11 because it hasn't been raised yet or at least has been
12 raised presuming that we've left it is the idea a
13 private right of action. So if we do want more cops
14 on the beat, we've heard a lot on this panel so far
15 about the costs of a private right of action in
16 privacy laws, and not so much about sort of the way in
17 which that puts a different kind of cop on the beat,
18 even if it does also make companies terrified.

19 MR. HO: Okay. So, I'd like to focus on the
20 -- continue our focus on US laws. And David had
21 mentioned COPPA earlier, and so here in the US, we
22 have a number of privacy laws that cover conduct of
23 entities that collect certain types of information,
24 such as information about consumers' finances or their
25 health. Various statutes address personal health

1 data, financial information, children's information,
2 contents of communications, driver's license data,
3 viewing -- video viewing data, genetic data, and, you
4 know, the list goes on and on.

5 But I guess the question here, are there
6 gaps that need to be filled with respect to certain
7 entities or certain types of data or conduct and why?

8 MR. HEYDER: Yes.

9 MS. WATSON: Yeah, I mean, I think the
10 answer to that question is yes. But I do think we
11 should acknowledge that the sectoral approach that we
12 have in the US sort of developed at the right pace at
13 the right time, and so we targeted areas that were
14 sensitive like financial information and health
15 information and children's information, and so the FTC
16 has capably demonstrated its ability and force in
17 those areas.

18 But I think we've seen the marketplace
19 evolve, and so there are now blurred lines in many
20 ways. So there's been a blurring of the distinction
21 between what's personally identifiable information and
22 what's not, right? And so -- and now there's just
23 this spectrum of information that can lead to sort of
24 sensitivity and very fast.

25 We've also seen blurred distinctions among

1 entities with the diversification of their business
2 portfolios. And we've seen blurred distinctions among
3 industries, and so more and more companies that are
4 traditional brick-and-mortar or in manufacturing are
5 embracing technology. And so we have a blurring of
6 distinctions in myriad of ways, and as a result of
7 that, the framework that we've set is no longer fit
8 for purpose.

9 And just to use as an example with respect
10 to HIPAA, you know, that is an -- a law that applies
11 to protected health information and certain healthcare
12 providers and business associates, but there are a
13 number of ways in which a person's medical information
14 is not going to be part of that coverage, right? And
15 so to the extent a consumer is uploading their own
16 information on a platform and there's no healthcare
17 provider, it would fall outside of HIPAA. HIPAA also
18 pertains to electronic billing records. So are we
19 talking about consumers that are paying in cash? And
20 not to mention the number of health-related apps that
21 sort of would fall outside of HIPAA as well to the
22 extent that the covered providers aren't involved.

23 And so -- and when we talk about this
24 spectrum of information and whether it's sensitive,
25 you know, so our view of sensitive data is it would be

1 medical information, right? But even that health
2 information that falls outside of HIPAA is still
3 personal information that's not protected by that
4 sectoral law.

5 And so I think that's one example where
6 there is a gap. There's obviously many more. And
7 that's why we believe a comprehensive federal law is
8 necessary both to provide that coverage and also to
9 ensure that all companies and all industries are
10 engaging in sound business practices when it comes to
11 consumer privacy.

12 MR. CATE: And it's not just gaps, it's
13 overlaps as well that are the huge problem. So why
14 should it matter when I test my blood sugar whether I
15 do it in -- using a medical device and it's covered by
16 HIPAA or I use my iPhone and it's not covered by
17 HIPAA, or I pay for my hospital bill and it's covered
18 by HIPAA but when the credit card charge goes through,
19 it's not covered by HIPAA.

20 This makes no sense to individuals who use
21 data in a pretty seamless, global way around ourselves
22 that all of these different laws abut or may not
23 actually abut or in some cases actually overlap.

24 MR. HO: And Markus?

25 MR. HEYDER: Thanks. So I agree with

1 everything Shaundra and Fred just said. To the extent
2 we need some sector-specific focus and expertise and
3 more detailed elaboration around certain rules, I
4 mean, I think we could draw, you know, from codes of
5 conduct and certifications and use that mechanism to
6 provide that kind of framework where it's needed.

7 But otherwise I agree, we need a
8 comprehensive baseline approach to privacy that covers
9 all sectors pretty much equally.

10 MS. MOY: I do want to just highlight this
11 problem that we are running into, though, that
12 Shaundra was just touching on, that the distinction
13 between information that we might have previously
14 classified as sensitive and other information is
15 rapidly disappearing if -- or, you know, or I
16 shouldn't say disappearing, but is becoming less of a
17 clear distinction, right?

18 I mean, one can infer information about
19 whether or not a person has Parkinson's from sensors
20 on the phone that might detect a tremor in a person's
21 hand, right? One can draw inferences about location
22 of an individual from information about the
23 individuals around them, right? From Mac addresses of
24 nearby devices, information that we might not think of
25 as historic -- as traditional location information.

1 Again, accelerometer and other phone sensor
2 information, those can reveal information about -- not
3 just about location but also about activities that an
4 individual is participating in. And that's one of the
5 reasons that it's important for us to focus not just
6 on in the future protecting certain classes of
7 information but also in ensuring that there are
8 guidelines up that prevent information from being
9 used, information about consumers from being used in
10 ways that we find concerning.

11 So, if we would have found health
12 information -- it concerning to use health information
13 about an individual to target advertisements -- to
14 target employment advertisements to that individual,
15 then we might want to prevent other information about
16 an individual that could be used to infer health
17 information from being used to target those types of
18 advertisements, right?

19 I mean, we might need to start thinking
20 about how discrimination or other harmful data uses
21 could flow from information that isn't historically in
22 the sensitive bucket and focus on preventing some of
23 those uses.

24 MR. LEDUC: And that's absolutely the focus
25 of the NAI is to prevent certain types of data use for

1 advertising and to prohibit some of these sensitive
2 areas, but I think, you know, taking a step back, I'd
3 like to build onto the conversation talking about
4 personal information. I mean, we are at a -- at a
5 point where we've got this expansive definition
6 seemingly broader with every new bill in the CCPA.

7 I mean, I think a couple of people have
8 touched on that already today how it's just so
9 incredibly broad to roll in everything. So and what
10 the impact of that is, unfortunately, I mean, I think
11 the previous panel, one of the previous panels where
12 Jules was talking about different types of de-
13 identification and use of pseudonymous data I think is
14 lost on a lot of policymakers today, the notion that
15 you can get good protection from certain types of --
16 around certain types of data, the use of pseudonymous
17 data that is not personally identifiable, identified
18 tied to a consumer that is applied and used with
19 certain controls, technical administrative controls,
20 legal controls, is a privacy gain. It's a big privacy
21 benefit.

22 And it's one that we are very proud to have
23 helped deliver in the advertising space, but this is
24 the type of thing that we need used throughout the
25 data ecosystem is we need to rely on this type of data

1 as much as possible. And we need laws that are going
2 to actually encourage that rather than discouraging it
3 by just creating a giant bucket and saying, well,
4 everything is personal data, everything is in the same
5 bucket and, therefore, you have to treat it absolutely
6 the same way. And it's all very -- you know, clearly,
7 clearly, a lot of this data can be re-identified.
8 We're long into the era of big data and
9 supercomputing, and we're going to go further down
10 that path, but we need to be able to rely on certain
11 practices, privacy protection practices, rather than
12 just sweeping everything together.

13 MS. VANDRUFF: So, we've gotten a number of
14 interesting questions from our audience, and I want to
15 -- Jared and I would like to take an opportunity to
16 ask a few of them. And the first that I'd like to put
17 to our panel is about regulatory sandboxes. So, at
18 the outset, just what do you think about regulatory
19 sandboxes? But more granularly, is there precedent
20 for doing it? And how can it be done effectively
21 without giving companies a free pass?

22 MS. KAMINSKI: So this was a term or a
23 process that I was less familiar with before I spent
24 time in the EU. I think it's interesting to think
25 about the notion of a regulatory sandbox in --

1 MS. VANDRUFF: And can I just interrupt you?
2 I'm sorry, Margot.

3 MS. KAMINSKI: Sure.

4 MS. VANDRUFF: Can you define for the
5 audience what that means?

6 MS. KAMINSKI: Effectively a regulatory safe
7 space for an industry -- a nascent industry to play in
8 like my toddler --

9 (Laughter.)

10 MS. KAMINSKI: -- while it's trying to
11 figure out -- while the regulator is trying to figure
12 out what the harms are and what the regulations should
13 look like, so this is related to the concept of safe
14 harbors but with a little bit more, I would say,
15 proactivity on the part of the regulator in just
16 deciding this is a space in which we want to sort of
17 have a light touch.

18 And, again, I think the tension here is
19 exactly again what Fred brought up earlier of you need
20 to have vagueness in some ways, within the law for a
21 regulator to be able to do that. You risk the
22 possibility of capture if you do that. On the other
23 hand, it does make the discussion of harms and
24 concerns about an industry much more concrete than if
25 you just full-stop employ a precautionary principle

1 and don't let the industry operate and decide just to
2 regulate it out of existence or alternatively more the
3 US approach of not regulating it at all until you see
4 concrete terrible harms impacting millions of people
5 across the United States.

6 MR. CATE: I would just say I'm a huge
7 believer in the regulatory sandbox, but we've been
8 doing it for decades in the United States. It's
9 nothing new. For years, it was possible to come to
10 events like this, you ask questions, you get
11 responses. If you disclose something incredibly
12 revealing, you know it could possibly be used, but on
13 the other hand, it's not generally the way that
14 federal agencies go out looking for information.

15 And I think they're also, to some extent,
16 being oversold in some of the new environments in
17 which they're being developed, which is the same
18 principle is going to apply there. If I go into the
19 Information Commissioner in the United Kingdom and I
20 disclose something that's actually threatening to
21 humans, I'm just guessing they're not going to say,
22 well, it was a sandbox, we don't really care, we'll
23 just wait until we hear about it from somebody else.
24 They're going to say let's follow up on that right
25 now.

1 I think the point is that regulators serve
2 multiple roles. And, again, the FTC has more
3 exposure, more experience at this than anyone. And
4 one of those is being able to participate in a
5 dialogue where you get advice and the advice of others
6 and you get feedback as opposed to just a subpoena
7 telling you that now you're in trouble.

8 MR. HO: Actually, so, we're running short
9 on time, and I want to give everyone their minute or
10 two at the end to give their closing thoughts. So I'm
11 just going to ask one more question that we received
12 from the audience.

13 So we've been talking about the roles of
14 state AGs when it comes to privacy enforcement, and as
15 other states pass CCPA-like laws with added AG
16 rulemaking, are state AGs the appropriate agency to
17 provide rulemaking guidance and enforcement? Do we
18 need something more akin to EU DPAs?

19 MR. LEDUC: Well, I mean, I think -- I don't
20 think we're doing very well with the EU DPAs, or at
21 least so far. I mean, I think that that's the threat
22 we face, right? I mean, whether it's through -- I
23 would think through -- mainly through a state model
24 but certainly not a federal model to empower different
25 decisions by different state ags.

1 I mean, I think it's fair to say that no --
2 I mean, looking at a state legislative landscape and a
3 patchwork approach, no one is well served -- not
4 consumers, not businesses -- by having different
5 privacy -- you know, different standards in different
6 states. So I think we -- I mean, I think as a
7 practical matter, we can dispense with that.

8 Having AG enforcement, as I mentioned, is a
9 real, I think, benefit to the FTC, but in terms of
10 having rulemaking authority and the ability to, you
11 know, interpret the laws, frankly, if we were to kick
12 that to AGs just -- and let them all make decisions, I
13 think we would be back and we'd have just a disparate
14 set of decisions that would look a lot like if we had
15 a patchwork of different legislation.

16 MS. MOY: I just want to push back a little
17 bit on the idea that a patchwork is always bad because
18 I think that -- you know, I mean, from a consumer
19 perspective, a strong patchwork is better than a weak
20 federal standard, right? You know, so -- and if you
21 look at data security and breach notification, for
22 example, you know, we do kind of -- we have this
23 patchwork of state laws, if you will, and although
24 there are, of course, complaints about that -- it's
25 not universally loved -- it offers a lot of benefits

1 to consumers. One of those is legislative agility.

2 Between 2015 and 2018, I think 23 states
3 updated their data security and breach notification
4 laws. That's a lot of activity. A lot of those
5 updates happen because state AGs have contact directly
6 with both companies and consumers, see a shifting
7 landscape and make recommendations to the state
8 legislature that it respond to shifting threats.

9 So one of the big things that happened is
10 that a lot of states updated their laws to cover
11 health information, not just health information
12 collected by healthcare providers but maintained by
13 other types of entities as medical identity theft was
14 on the rise. So there is sort of this -- there's this
15 legislative agility function that having state
16 legislatures and, if you will a patchwork of state
17 laws, that does serve consumers in many ways.

18 MS. WATSON: I think I would just add,
19 though, just the premise, I think we want to see a
20 strong federal law, and so I wouldn't assume away the
21 fact that a federal law would be weak. I think we
22 think of sort of replacing state laws is appropriate
23 if we are able to craft a robust and strong federal
24 law.

25 And the other thing is on a data breach

1 notification piece, that's obviously been a
2 significant challenge for businesses. But I think
3 that problem is magnified when you talk about sort of
4 these broader privacy issues when you're going to the
5 heart of the architecture and what companies are doing
6 and how they share data. And so I think that's a
7 little bit of a different animal than this piece of
8 notification because the coverage is so broad and the
9 impact is so significant.

10 And so I do think that the different and
11 conflicting obligations would present a significant
12 challenge, and it's not just about sort of what
13 companies -- the obligations that they provide, it's
14 also what consumers expect. And so I just think a
15 better approach is to have one national standard that
16 provides clear expectations for consumers and clear
17 obligations for businesses, but you know, I do agree
18 that that should be in the form of a strong federal
19 law, not a weak one.

20 MS. VANDRUFF: So, Shaundra, you've given me
21 the perfect opportunity to ask --

22 (Laughter.)

23 MS. VANDRUFF: -- our last question of the
24 panel, which is, you know, we talked over the course
25 of this hour-plus about different frameworks and what

1 different bodies have done to tackle privacy.

2 I guess the question is, you know, what --
3 if we were to take different parts from different
4 privacy frameworks that we've been discussing today
5 and that you all have studied in your academic work
6 and in the course of representing your various
7 clients, what should a federal privacy framework look
8 like? What part of existing law such as the CCPA or
9 GDPR or other state law should we use as guideposts?
10 And I'd ask each of you to just take a minute or so to
11 address that question. And, Shaundra, you started, so
12 you get the first swing at this.

13 MS. WATSON: Sure, sure. So our member
14 companies think a federal privacy law should include
15 three key components. The first is to give consumers
16 the right to know and the right to control what
17 happens to their personal information. The second is
18 to impose obligations on companies to safeguard
19 consumer data and to prevent its misuse. And,
20 finally, we believe there should be strong,
21 consistent, and effective enforcement.

22 MS. MOY: So I'll say -- so I think a couple
23 things that I would take from GDPR are data
24 minimization and purpose limitation and powerful
25 fining authority from CCPA. I probably would take

1 state AG enforcements, but then I also think that it's
2 really important that we see rulemaking authority to
3 ensure fairness in automated decision-making and to
4 prevent things like discriminatory advertising, not
5 just eligibility determinations but advertising of
6 opportunities. And a private right of action in no
7 small part because historically disadvantaged
8 communities have not historically always been
9 protected by agencies when agencies are expected to
10 protect everyone.

11 MR. LEDUC: Well, as some of you may have
12 heard, we formed a coalition yesterday and announced
13 an effort to promote legislation, and it echoes -- you
14 know, what I've said today really echoes that
15 movement, and it's really largely focused on the
16 notion of enforcing around reasonable and unreasonable
17 data practices, picking up on what Laura said,
18 creating clear categories and uses that are
19 unreasonable and those that are reasonable and
20 building in an opportunity for co-regulation,
21 expanding the authority, expanding the resources of
22 the FTC and giving them some -- I mean, I think some
23 appropriate authority, creating a new bureau of data
24 protection to be able to enforce around this notion of
25 what is unreasonable.

1 I mean, I think the FTC did some really good
2 work over the last couple years under acting Chairman
3 Ohlhausen, really assessing informational injuries.
4 And I think we could all define them differently. I
5 think we can all agree they're nearly impossible to
6 clearly define, but we need to protect against those
7 practices, those bad practices. So a framework that
8 can really help us do that and let us be able to use
9 data for good purposes, promote innovation, and
10 continue doing things that consumers want.

11 MR. HEYDER: So we need a comprehensive
12 baseline privacy law. We think it should be based on
13 the concept of organizational accountability. It
14 should take the risk-based approach. It should employ
15 codes and certifications to outsource, so to speak,
16 some of the functions that otherwise would belong to
17 the FTC. There should be strong enforcement powers by
18 the FTC.

19 I think, ultimately, we should use the
20 accountability model to move away from the situation
21 that was discussed in the earlier panel where
22 everything's about consumer expectations, secondary
23 uses that you can pick and choose from and where you
24 control everything that happens to your data.
25 Instead, we want to create a system where every

1 organization that touches data is sort of tied into
2 this organization -- accountability framework that is
3 enforced against them and that enables consumers not
4 to worry about secondary uses that are otherwise
5 beneficial for society and for themselves.

6 And for organizations that are implementing
7 accountability to focus on risks and harms and to have
8 an obligation to prevent those. So to free up
9 consumers from having to be engaged every day, every
10 single day on what happens with the data and what
11 doesn't happen. There's a place for consent and for
12 making choices, and I fully agree with some of the
13 examples that were given, but for the most part, as
14 Fred had suggested earlier, that's no longer possible
15 and feasible.

16 Finally, a US policy framework should be
17 interoperable as much as possible with other
18 frameworks like the GDPR for consistency purposes
19 to -- that would benefit companies in terms of
20 implementation. It would help regulators in terms of
21 enforcement and would help consumers in terms of
22 providing consistency across the globe.

23 But this interoperability or alignment with
24 other models should not come at the expense of
25 undermining the US's ability to continue to innovate

1 and to work with data effectively, and that should be
2 protected and that should be part of the goal of any
3 new privacy law.

4 MR. CATE: I feel sort of lonely up here.
5 Everybody has a "we" that they speak for. And I don't
6 know, Margot, do you? Margot and I just speak for all
7 rational people everywhere --

8 (Laughter.)

9 MR. CATE: -- and we think -- I think there
10 are really six elements that should be key here and
11 one is put consent back in a box. It should not be
12 the dominant focus. It's not rational. It's not
13 usable. It's not workable. And it's frankly not fair
14 to individuals to say that we're going to be held
15 responsible for the effects of decisions we may not
16 even know we're making, even though we can't possibly
17 understand what those effects are going to be.

18 Two, I would focus a lot less than US law
19 has historically done and certainly than European law
20 does on collection and much more on use. What we've
21 learned, especially in the area of government
22 collection of data, there's always a legitimate reason
23 to collect it. There is always a legitimate use. You
24 need it for a credit card transaction. You need it
25 for online. You need it for dealing with a doctor.

1 You need it someplace.

2 And what we don't want to limit our focus on
3 is the terms under which it's being collected but
4 rather what is it being used for and, more
5 importantly, what is it being reused for and how is it
6 being used in ways that may be shocking or potentially
7 harmful.

8 Third, accountability, which I think Markus
9 has been eloquent on, but again the notion of
10 responsible stewardship of data and that we expect
11 organizations that collect and use data to do so in a
12 way that is responsible and that they will be
13 accountable when those data cause harm.

14 That suggests the fourth, which is what the
15 Europeans call a risk assessment model, but basically
16 a harm-based model, that that should be the focus.
17 We're not trying to nail down everything. We're
18 trying, like most consumer protection laws, to prevent
19 harms that can be prevented. And there's a lot that
20 we agree are harms, and then that leaves an area where
21 folks can rationally disagree and courts might play a
22 role.

23 Fifth, vigorous federal enforcement and a
24 federal regulator. I personally think that should be
25 the Federal Trade Commission, but it would mean a lot

1 more staff, and it would clearly mean rulemaking
2 authority. It's not sufficient to say after the fact
3 what's been done wrong.

4 And, finally, remembering what I'm now going
5 to call the Heyder Principle, and that is on the other
6 side of this balance are the extraordinary benefits we
7 get from the widespread use of information. And
8 they're important economically. They're important
9 personally. They're a foundation of a good part of
10 the 21st century economy, and people love those
11 benefits and expect those benefits, and so we should
12 keep in mind this is a balance at all times. It is
13 not a single focus issue.

14 MS. KAMINSKI: I have 17 seconds to say my
15 concluding thoughts on this. And I think that largely
16 we'll be agreeing on a lot of the high principles and
17 disagreeing on some of the probably most important
18 decisions. And those things that are the focus of
19 most disagreement include both the issue of preemption
20 and the issue of private rights of action.

21 The second sort of substantive category I
22 would add in there -- we didn't get time to talk about
23 today -- but where I agree that focusing only on
24 notice and choice is a very limited way of looking at
25 privacy and, in fact, in practice has been

1 individually disempowering. There are elements of
2 individual empowerment that I think are important, and
3 principles about data collection that are also
4 important that exist in the EU regime and don't exist
5 here.

6 So in the CCPA, we don't really see, as I
7 said, much in the way of purpose limitation, purpose
8 specification, and use limitation principles. We
9 don't see data minimization principles, and the use
10 case I'd like is to try to think through a little bit
11 when we're trying to find points of disagreement
12 rather than agreement is the idea of monitoring of
13 biometric information in public spaces. I think that
14 teases out a lot of the divides potentially in these
15 communities.

16 Very last, I promise, we've long seen a
17 hybrid state/federal regime where we can conceive of
18 data privacy, or I guess privacy more generally as
19 being simultaneously a global federal issue and a
20 highly localized issue. And as we move to a world of
21 smart cities and CCTV-monitored public spaces, states
22 and even municipalities really do see those concerns
23 as being issues that are subject to their purview and
24 even local police powers. Thank you.

25 MR. HO: And thank you. Please give our

1 panelists a round of applause.

2 (Applause.)

3 MR. HO: And with that, we'll start our
4 break. And please return promptly at 3:45.

5 (Recess.)

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 CURRENT APPROACHES TO PRIVACY, PART 2

2 MS. JILLSON: Welcome back, and if you would
3 all just take your seats, we have one more panel
4 discussion this afternoon.

5 So before the break, we had the first part
6 of the current approaches to privacy, and for our last
7 panel discussion today, we have Current Approaches to
8 Privacy, Part 2. And what we will be doing is trying
9 to take some of the broad principles that we talked
10 about before the break and make this a little bit more
11 concrete. So we're going to be walking through five
12 hypothetical scenarios in which these panelists are
13 going to be trying to tackle specific problems and try
14 to unpack how would CCPA deal with this problem, how
15 would GDPR, how would the US sector-specific approach.

16 But before we get into the substance of
17 that, let me take just a moment to introduce myself,
18 my comoderator, and our esteemed panelists today. My
19 name is Elisa Jillson. I am an attorney in the
20 Division of Privacy and Identity Protection. My
21 comoderator is Andy Arias, also an attorney in the
22 Privacy Division.

23 And here today, we have Lothar Determann,
24 who is a Partner at Baker McKenzie; Jay Edelson, who
25 is the Founder and CEO of Edelson PC; Rebecca S.

1 Engrav is a Partner at Perkins Coie; Alan Raul is a
2 Partner at Sidley Austin, LLP; and Tracy Shapiro is a
3 Partner at DLA Piper.

4 And so how we're going to start off with our
5 panel today is Lothar is going to tackle our first
6 hypothetical. He's going to take a few extra minutes
7 to kind of lay some groundwork on some of the key
8 differences between CCPA, GDPR, and other laws. After
9 he takes that first crack at the hypothetical, we'll
10 open it up for discussion with the rest of the
11 panelists, and then we'll be moving along to the next
12 hypothetical.

13 So with all of that said, I'll hand over the
14 clicker to Lothar, and thank you very much for taking
15 us to the very first hypothetical. And I'm sorry, if
16 you could click the slide one forward, I'll just read
17 the hypo, and then we'll get started.

18 So Company A, a US startup with a German
19 subsidiary, offers a newsletter for cycling
20 enthusiasts with information on safety, health, and
21 new cycling products. It's funded through ads. It is
22 developing a new product that can sense danger, such
23 as weather changes or drunk drivers, and warn
24 cyclists. Health insurance companies, automakers, and
25 city planners seek access to its data.

1 One day, an engineer inadvertently accesses
2 a file containing name and health insurance provider
3 for 200,000 employees and newsletter subscribers.

4 Lothar, what are the implications for this
5 company's practices under various legal regimes?
6 Please walk us through that.

7 MR. DETERMANN: I will walk you through, and
8 I'll lay the groundwork, too, that you invited me to
9 lay. Thank you so much for inviting me. It's
10 wonderful to be in DC, particularly at cherry blossom
11 time. And I agree with Commissioner Phillips
12 wholeheartedly that it was a fantastic set of
13 panelists today, and I very much enjoyed this today
14 and tomorrow, what I've heard, and I'll try to lay a
15 little bit of this groundwork and apply the insights
16 and the broad principles and the purposes of different
17 approaches to privacy law for our panel, which is now
18 going to apply this to concrete hypotheticals.

19 The current approaches to privacy law vary
20 from country to country based on different needs and
21 preferences of people or governments, for information,
22 for human dignity, security, privacy, freedom, and
23 technological innovation. Let's start with Europe,
24 the old country. We heard to protect privacy and
25 prevent George Orville's vision of 1984, the European

1 countries regulated data processing as such, with a
2 prohibitive and bureaucratic regime.

3 European countries prohibited data
4 processing by default. And companies and governments
5 must not collect, use, share personal data except as
6 specifically permitted. The basic idea was the less
7 we use computers and data, the better for data
8 privacy. This is from the 1970s. This was harmonized
9 in 1995. The question was raised what the purpose
10 was. It was a trade measure to enable free flow of
11 information within Europe and cut off flow to other
12 countries. That was the '95 directive, and that idea
13 of the free flow of information in Europe for economic
14 development is still in the GDPR.

15 So what happened through the '70s, European
16 citizens embraced information technologies made in the
17 US, increasingly in Asia, the same compromise on
18 privacies elsewhere. Where the European governments
19 were constrained by data protection laws and
20 intelligence gathering, foreign governments, including
21 the US NSA, stepped in. And where the European
22 companies were hindered in developing information
23 technology products by this data processing
24 regulations, US companies stepped in.

25 Effective May 2018, the EU GDPR doubles down

1 on this approach of the '70s with even more
2 prohibitive data processing regulation and large fines
3 that are intended for US tech companies specifically
4 as publicly stated. Additionally, the German
5 Government came up with creating property rights in
6 mobility data to protect the local auto industry from
7 competition, which underlines that one of the purposes
8 of privacy and data protection law is also trade.

9 Now, we already heard about the US approach,
10 very different path. Data processing, as such, is
11 allowed and we have focused on harm sector situations,
12 specific privacy laws that are constantly updated,
13 supplemented, and are actually enforced, which has not
14 been true in Europe for much of the 50 years of
15 history there.

16 We have in California the first data
17 security breach notification law worldwide, 2002. It
18 took the Europeans 16 years to follow this. We had
19 the first law requiring privacy notices for websites,
20 2004. We have dozens of other privacy laws. We have
21 one for supermarket club cards. We have one for RFID
22 tax. We have one for automated license plate
23 scanners, and that's important to understand when CCPA
24 is sold as an omnibus law, it's just one of literally
25 dozens of laws in California, alone in one state of

1 the United States.

2 I believe these laws have effectively
3 protected individual privacy against newly emerging
4 threats while allowing technology to thrive. And the
5 FTC has done its part in developing a body of data
6 privacy and security law that is focused on preventing
7 consumer harm, but after enacting laws for 50 years,
8 situation-specific, and without repealing,
9 harmonizing, or updating the existing laws and
10 streamlining them, simplifying them, the US are now
11 also suffocating innovation and business.

12 The California Consumer Privacy Act against
13 data sharing overburdens companies with excessive,
14 complex, rigid, and prescriptive requirements. If
15 other states follow and Congress does not preempt,
16 only the largest of companies will be able to handle
17 compliance.

18 Now, let's look at Asia a little bit, too.
19 I'm at the West Coast. We don't just look to Europe.
20 The Asian countries strongly encourage and support
21 data-driven innovation. The People's Republic of
22 China focuses its data laws not on individual privacy
23 but on data residency requirement, internet
24 censorship, and protecting Chinese-owned companies
25 against foreign competition.

1 China mandates Chinese companies to develop
2 and apply artificial intelligence, big data analysis,
3 social scoring, and we see other countries taking
4 their own path. India is following a hybrid approach
5 combining the Chinese and Russian data residency
6 requirements with European data processing regulation,
7 but most of the other countries are more or less
8 following the European data processing regulation
9 approach, at least on paper.

10 If the United States also follows the
11 European approach and regulates data processing with
12 GDPR-like law, established multinationals will
13 appreciate and benefit from international
14 harmonization for sure, but startup companies will be
15 hampered and innovation will slow. This will hinder
16 progress in autonomous vehicles, artificial
17 intelligence, and, as we heard on one of the previous
18 panels, in the healthcare sector. I believe it will
19 be literally unhealthy.

20 If the United States follows Europe or stays
21 on its current course and fails to streamline and
22 harmonize its myriad privacy laws, I expect that
23 global innovation leadership will move to Asia. In a
24 few years, US citizens will then be using technologies
25 made by Chinese companies, and the impact on

1 individual privacy, national security, and the economy
2 in the United States would be similar as in Europe
3 since the '70s, and in that sense I think we should
4 and can learn from the European approach, which will
5 now apply to our hypotheticals.

6 We start with the hypothetical that Elisa
7 just read and take a look at the benefits that this
8 company offers to consumers and the risks to privacy.
9 The benefits include global, local information free of
10 charge for cyclists. I'm a cyclist enthusiast. I
11 appreciate this greatly. And it is developing life-
12 saving new cycling safety technologies, which are very
13 much needed. As healthy as cycling is a danger it is.
14 And it offers attractive jobs in the technology
15 sector.

16 Now, there are risks. They include, as we
17 heard the previous panel and the first panel today and
18 also in the ninth session December 12 from Professor
19 Solove, discrimination by employers, insurance
20 companies based on habits, health condition is
21 embarrassment, fraud, stalking, and many other harms
22 that we should definitely take into account.

23 Now, how do these different approaches to
24 privacy now have an impact on this company in our
25 hypothetical? The EU GDPR does not, contrary to

1 common belief and as often emphasized as an opt-in
2 law, would not require this company or its German
3 subsidiary to obtain consent from consumers. European
4 companies can and often must rely on alternative means
5 of justifying the data processing against this general
6 prohibition of data processing and rely on things like
7 necessity-performed contracts or legitimate interests
8 that are not outweighed by the overriding interests of
9 the data subjects.

10 The GDPR, as broad as the prohibitions are,
11 as broad and vague are some of the exceptions, but the
12 GDPR also puts a lot of paperwork obligations and data
13 minimization on our company. It asks the issue of
14 very specific notices that are different and have
15 different requirements. They're not really compatible
16 with the kind of notices that the FTC requires, which
17 have to be understandable by consumers, not possible
18 with the details required for 12 to 13 GDPR.

19 They have to satisfy data access portability
20 deletion requests free of charge to individuals but to
21 the public and community appointment of a data
22 protection officer, designation of a local
23 representative for the US company, data protection
24 impact assessments, documentation to demonstrate. It
25 goes on and on, particularly also to satisfy the

1 international transfer restrictions that are
2 specifically benefitting the European companies and to
3 the disadvantage of foreign companies.

4 Compliance is very expensive for the startup
5 company, and these requirements are not focused on any
6 particular harm as was noticed on the previous panel.
7 The privacy harms are not core and center. It just
8 discourages data collection on this idea the less data
9 collected the better for data privacy.

10 Now, the CCPA does its own part here. It
11 doesn't prohibit anything. There's no data
12 minimization in there. But the CCPA will require, in
13 conjunction with other California laws, very specific
14 and elaborate disclosures that are not compatible with
15 other US laws or the GDPR. Companies, if they want to
16 share data with other companies in certain
17 circumstances, have to put a special link on their
18 website that says "your California privacy rights."
19 They have to put a link under the CCPA for do not sell
20 my personal information, and if every state in the US
21 and every country does that, then all the websites and
22 the mobile pages of the world will be full and we
23 won't put any other content on them.

24 Also, the California residents may opt out
25 of information selling but remain entitled to service,

1 which we heard on a previous panel will cause
2 companies to start charging for services that are now
3 available for free, which will take one important
4 consumer benefit away.

5 Residency requirements in countries such as
6 Russia, China -- in India the bill is pending.
7 Indonesia and Kazakhstan will require our startup
8 company to establish a local presence to keep all data
9 there so it's accessible to the local government,
10 which startup companies often can't afford to do.
11 Plus, in China, a company that is not Chinese-owned
12 can't do much over the internet anyhow under the
13 regulatory regimes.

14 Perhaps the biggest impact for our company
15 that wants to develop this safety device, though --
16 and this one is not about advertising as pretty much
17 all previous panels were focused on -- is to develop
18 the sensors and train the self-learning algorithms
19 they need to collect data on public places, on public
20 roads. They don't need identifying information, but
21 they need data on what a person looks like, sounds,
22 smells, acts, and so on.

23 And this is personal data under European
24 law, personal information under the CCPA, and
25 companies should be able to exchange this information

1 with other companies, otherwise, every single company
2 has to drive around everywhere to collect this
3 information. But the GDPR makes this extremely
4 difficult and nearly impossible for a company in
5 another country due to the restrictions on special
6 congratulations of personal data. You have to get
7 consent for transfer to the US, which is impossible.
8 You can't drive around on the street and then get
9 parental consent inviting from a kid that happens to
10 be on the camera.

11 Similar, the CCPA requires opt-in consent
12 from teenagers and also parental consent for minors,
13 which is just not practical. So these technologies
14 will not be developed with input in California, with
15 data from California. In China, the activities are
16 encouraged by the government for Chinese companies.

17 Now, the second part of our hypothetical is
18 one that illustrates a slightly different point.
19 That's the data security breach. And we heard on the
20 previous panel what a hard time companies have when
21 they're faced with such a situation. I think the
22 practitioners on the panel will agree. You have to
23 look at 50 different state laws, plus different
24 countries' laws, to determine who you have to notify
25 in Europe, in what language, what regulator has to be

1 notified in 72 hours. And that adds a huge compliance
2 burden.

3 Plus, on top of it, if this list with just
4 people's name and the name of their health insurance
5 company is law, then everyone on that list is entitled
6 to between \$100 and \$750 statutory damages under the
7 California law without any showing of harm.

8 With this hypothetical, I mean to illustrate
9 just a few points, namely, that the broad prohibitions
10 on data processing and also data minimization cause
11 too much collateral damage and don't do enough for
12 privacy. The data genie is out of the bottle. The
13 data is everywhere. We need to focus on the harm that
14 it causes and specifically legislate that.

15 As we heard on the previous panel, if
16 discrimination is the problem, then we need to
17 prohibit that form of discrimination and act on it and
18 enforce and not just prohibit every data sharing and
19 collection.

20 The data processing regulations in Europe
21 have been largely ineffective. The GDPR is not a
22 modern law. It's 50 years old. It's doubling down.
23 And similar threats follow from the excessively
24 prescriptive and complex disclosure requirements and
25 data subject rights like the CCPA, particularly since

1 that is one law for 50 states.

2 Diverging disclosure breach notifications
3 and other requirements on the state level hamper
4 interstate commerce, should be harmonized nationwide,
5 and I personally believe the United States and the FTC
6 have been on the right track to focus on consumer harm
7 and individual privacy, but they do need to now
8 streamline and harmonize existing laws so that
9 organizations, particularly smaller businesses, can
10 realistically understand and comply with privacy laws.
11 Otherwise, these laws will be counterproductive if
12 nobody can follow them anymore.

13 I'm looking very much forward to our
14 discussion after this little bit of groundwork.

15 MS. ARIAS: Lothar, thank you very much for
16 that. So let me open it up to the rest of the
17 panelists. Lothar did a very good job of kind of
18 detailing some of the issues with this hypothetical,
19 but I'm curious if you all have any other thoughts
20 about maybe some of the issues that he may not have
21 been able to cover that kind of pop into your minds.

22 MR. EDELSON: Yeah, I'd be happy to jump in.

23 MS. ARIAS: Jay, please.

24 MR. EDELSON: So I come at this from a
25 totally different perspective. I'm on the plaintiff

1 side. I represent class actions and also regulators
2 at the state, city, and county level. The first
3 thing, it was interesting to hear that if we have
4 strong privacy laws, then it's going to stifle
5 innovation and everything's going to go to China. I
6 think that that -- that's really not going to happen.

7 Let's focus on what most privacy laws are,
8 and those are consent laws. And that really for me,
9 the focus of the hypothetical has to start with that,
10 which is did Company A, did the startup get consent?
11 And it's really not hard to do. That's why I don't
12 think it's a huge burden. It's not going to stifle
13 innovation. All they have to do is say, "Here's what
14 we're collecting, and here's what we're going to do
15 with it."

16 Now, an issue which was brought up and it
17 also was brought up in previous panels was we've got
18 all these different laws -- there's federal -- I'm
19 going to focus on American law, the one thing that I
20 know about. I'll leave the EU to you. This idea that
21 if we have differing laws, we're all going to just --
22 it's too much to handle. First, for data breach
23 notification, I think it proves the opposite. We've
24 seen that companies have no problem complying with the
25 myriad data breach notification laws. Although, I

1 agree, having a uniform law there might be helpful.

2 With regard, though, to laws more generally,
3 if you look at what plaintiffs -- whether they be
4 regulators or private citizens -- sue under, they
5 generally start with consumer fraud statutes. So the
6 FTC will look under Section 5 of the FTC act. You'll
7 see state attorneys general will look at consumer
8 fraud statutes. When there are damages -- and can get
9 into what it means to be damaged -- private litigants
10 will look at consumer fraud statutes there.

11 And, again, the big issue is let's look at
12 what the public-facing statements are and compare them
13 to what actually is happening. And if there's a
14 mismatch, then that's when the company ought to be
15 held accountable.

16 MS. ARIAS: Anybody else on the panel have
17 any additional thoughts?

18 MS. ENGRAV: Just a small point. I think I
19 heard you correctly to state that in -- for the breach
20 part of the hypo that you would see a -- that this
21 would -- this would trigger under the CCPA and
22 potentially at the private right of action. And, of
23 course, none of this has been litigated yet. But
24 there is some language in that that I think might make
25 it such that, set aside for the moment whether it's a

1 reportable incident under existing California law,
2 that the private right of action wouldn't apply there
3 because some of the additional language there is
4 whether it's subject to unauthorized access and
5 exfiltration, theft, or disclosure as a result of the
6 business' violation of the duty to implement and
7 maintain reasonable security procedures and practices.

8 So I think maybe we just don't know yet. I
9 think we'd need to know more facts about this fact
10 pattern. How inadvertent was it? Were there good
11 procedures and practices in place? And so I think,
12 like, there just might be a little bit more going on
13 to that question.

14 MS. SHAPIRO: I would add the same thing
15 with regard to the health insurance question, that if
16 they start selling information to health insurance
17 companies, we'd want to know more, like, are they
18 advertising that as a purpose for the use? Are they
19 marketing the data? And in that way is there a Spokeo
20 situation? Is there a risk that they become a
21 consumer reporting agency because they're marketing
22 the data for purposes of making eligibility
23 determinations.

24 MS. ARIAS: Thank you. Okay, since our time
25 is short and we want to cover all the hypos -- we have

1 five hypos for you all -- we're going to go ahead and
2 cut the discussion here and move on to the next
3 hypothetical.

4 MS. JILLSON: So hypo two, Company B
5 develops a free mobile app with a location sharing
6 opt-in that offers shopping discounts based on
7 location. City planners interested in making downtown
8 shopping areas more "walkable" offer to pay for access
9 to the app's data.

10 And, Rebecca, perhaps you can start us off
11 with this hypo.

12 MS. ENGRAV: Sure. So I think for me it's
13 helpful to kind of take it into really concrete
14 questions in terms of is this okay or is it maybe
15 okay, depending on different facts. And I think it's
16 important to keep in mind that the hypo itself gives
17 us the concrete fact that the original location
18 sharing is opt-in. So we can all just assume that.
19 We don't have people who don't know that the location
20 data is being collected and they had a choice. It was
21 opt-in.

22 So as to the second part of it, though,
23 about can Company B share it with the city planners
24 when they offer to buy this data to kind of help solve
25 the problem of the dying downtown and retail, and they

1 want to see where do shoppers actually like to go and
2 kind of how do they walk through the city. If we take
3 it through these three different regimes, I think if
4 we -- well, we're going have to assume a couple of
5 things. We're going to have to assume that there's no
6 -- as Jay mentioned, of course, the first step in US
7 privacy law is what disclosures have been made and are
8 they true? So we can just assume that this isn't at
9 odds with any disclosures that have already been made
10 to consumers. So there wouldn't be an existing
11 deception issue.

12 If we assume that, then under US laws that
13 exist right now, in my view, kind of Section 5, the
14 state UDAP laws, there's no special law applicable to
15 this company. It's not in a regulated sector. So
16 there's no particular opt-in or opt-out requirement.
17 We're just in the land of general consumer protection,
18 be honest and accurate in how you describe your
19 product, and if you're not -- if this isn't at odds
20 with anything that they've said, I don't think there's
21 any particular opt-in or opt-out requirement.

22 If we then shift to CCPA, that's a more
23 interesting question there. CCPA, of course, does
24 have disclosure and opt-out -- not opt-in, but opt-out
25 -- required for sharing of data with a third party

1 when it's a sale. And here, the hypo is telling us
2 that it would be a sale because the city planners are
3 offering to pay for it. So if that's all that's going
4 on under the CCPA analysis, then consumers would have
5 a right, both to be specifically informed about this
6 and opt out of it.

7 I do think under the CCPA there is a
8 question that would come up about the fact that this
9 is a city getting the data. There are several
10 provisions in the CCPA that speak either to different
11 levels of law or to kind of just different aspects of
12 how governments might or might not either fall within
13 this, and here they're not even the subject, they're
14 the third party.

15 So I certainly haven't thought all that
16 through. I don't have an answer for you, but I can
17 definitely say in my look through CCPA preparing for
18 this I'm highlighting a lot of provisions that talk
19 about government and different aspects of levels of
20 law. And I think that there very well could be a
21 different answer under the CCPA for data sharing with
22 governments, as opposed to data sharing with other
23 private companies, even it's a paid exchange. And I'm
24 curious, actually, if others on the panel see the same
25 issue there.

1 But just to kind of close it out here on the
2 front-end question of do you need opt-in consent for
3 this, from a GDPR perspective, it's interesting, I
4 think we tend to think, oh, the GDPR is so protective.
5 EU is so much more conservative. You know,
6 interestingly, there's, again, no opt-in or opt-out
7 specific requirement here unless the company were
8 planning to rely on consent, which it likely wouldn't
9 because it's very rare to rely on consent because of
10 how onerous that standard is in the EU, they
11 presumably would be relying on a different legitimate
12 interest.

13 So long as you have a legitimate interest,
14 your obligations to provide transparency about what
15 that basis for processing is, but there isn't a
16 specific sort of opt-in or opt-out requirement. So if
17 -- so we've worked all that through. The company's
18 decided that, yes, they can share. They've checked
19 their disclosures. They know their privacy policy,
20 kind of it's great. It already says we share with
21 third parties.

22 A next kind of threshold gating question to
23 think about, I think, would be does it matter how many
24 subscribers this app has? And there we also do see a
25 little bit of a distinction from the CCPA, and there

1 are some really real practical questions for companies
2 about those triggering thresholds under the CCPA.
3 There's three of them. Do you have 50,000 California
4 residents? Or gross revenues in excess of \$25
5 million? Or at least 50 percent of your annual
6 revenue by selling the personal information of
7 California residents?

8 So this business, again, we don't know
9 enough facts, but depending on if they're based in
10 California, if this particular form of data sharing
11 and the money they earn from it is really their only
12 source of revenue, and/or it's a small app, so they
13 definitely don't have 25 million in revenue. I'm
14 making that up. So they may or may not come within a
15 CCPA-type law if there are these thresholds to it.

16 The existing federal regime, of course,
17 doesn't have any particular thresholds. GDPR also
18 doesn't have any particular thresholds. But that
19 could be another way where the regimes differ in how
20 they treat it. This app, interestingly, some apps are
21 going to have a real challenge figuring out where
22 their residents are located in terms of deciding which
23 ones they're going to decide, are entitled to CCPA-
24 type rights.

25 You know, that's a great benefit, actually,

1 of online services. And if you're doing a good job of
2 following your privacy principles of data minimization
3 and not collecting data you don't have, an app like
4 this may very well have user name and email address.
5 I mean, it's a pretty thin, simple app. So unless
6 they're just going to draw inferences from IP address,
7 they're not necessarily going to know where their
8 residents are located, unless they try to backtrack
9 from their location, collecting portion and saying
10 that anybody who walks in, you know, Menlo Park is a
11 resident of California. Visitors from Illinois, I
12 don't know how that would work out.

13 So I think the third piece that I'll talk
14 about then before we open it up to the panel is to
15 think about, well, what if the city has a breach. So
16 the city's received this data, kind of worked through
17 all the steps and, you know, the Company B was fine
18 sharing it. But the city doesn't have great data
19 security. They have a lot of turnover. Every time
20 there's a new administration, this is just a file
21 sitting around, and they have a breach. What happens
22 then?

23 Under existing law, location information
24 alone wouldn't trigger breach reporting in the United
25 States. In Europe, it might. The standard there

1 would be a substantial risk to the substantial rights
2 and freedoms of the data subject. And if you have a
3 lot of location information -- we also don't know from
4 this hypo if the city planner is seeing each of these
5 data points as just individual data points or if the
6 city planner knows that it's Person A making all of
7 those data points. We can't tell that from this. But
8 that distinction may make a difference to your
9 European breach reporting obligation there as well.

10 But as to who does the breach reporting,
11 that would also be an interesting question here if
12 it's a city planner breach. We've got kind of
13 existing, you know, that happens in the United States.
14 We already have plenty of fact patterns of where a
15 downstream vendor, a service provider encounters a
16 breach. They need to tell the first party from whom
17 they got the data, but it's the first party that would
18 conduct the breach reporting. Here, there could be
19 some interesting questions, depending on what time the
20 breaches happened in terms of ability to find the
21 folks and provide notifications.

22 MS. JILLSON: Well, thank you, Rebecca.
23 That's a great job spotting some tricky issues. We've
24 gotten an interesting question from our audience. If
25 the app says "we collect location information to

1 provide you discounts," is it a deceptive failure to
2 disclose under Section 5?

3 MS. SHAPIRO: I'll jump in on that. So I
4 think it's a very challenging question, and a lot of
5 my clients debate this issue with looking at the
6 Golden Shores case that the FTC brought, where there
7 was a flashlight app. They were collecting
8 geolocation information. There, they didn't say that
9 they were collecting it or sharing it, and there was
10 nothing in the privacy policy.

11 So I think there is this question of,
12 okay, if we're not that severe, and the consumer
13 expectations were such that you would never think that
14 your flashlight app is collecting location, but let's
15 say you've got an app where it is expected that
16 location would be collected, like here, it's clearly
17 disclosed that it is, do you need to have that sharing
18 in just-in-time disclosure, or can it be in the
19 privacy policy?

20 You know, the FTC has certainly said we want
21 it to be an opt-in for the sharing of location data,
22 and we want it to be just in time. But it was a
23 consent order. It's not binding law. But, you know,
24 do you want to be the company that tests that by not
25 following the Golden Shores order?

1 MR. RAUL: And I would add if this is taking
2 place in California, and with all the walking and
3 cycling going on and the CCPA, I'm sure everything is
4 taking place in California, there might be a CalOPPA,
5 the statute in California that requires privacy policy
6 disclosure for online collections of personal
7 information about California residents. And if that
8 doesn't include a disclosure of selling to the city,
9 there might be an issue there.

10 Another kind of off-the-wall issue here, you
11 know, we're kind of brainstorming here and free
12 association, is this is a city. Is surveillance
13 involved? And that's an issue that might be of
14 concern to people. And is the stored communications
15 act involved where if -- if they're a communications
16 provider, this app, which is sometimes an ambiguous
17 category, they would require, in order to provide the
18 information to a government agency, some kind of legal
19 process, like a subpoena, unless, of course, it were
20 with the consent of the walkers here.

21 One last comment is the ambiguity in
22 California for opt-in versus do not sell. So what if
23 they -- the people who are using this app opted in
24 specifically to all kinds of stuff, and then, you
25 know, California CCPA goes into effect, and they're

1 pushing "do not sell" buttons all over the place. Did
2 they really mean that? Did they really mean to
3 omnibus, don't sell when they want all these discount
4 coupons? So you know, we'll see how that -- how that
5 plays out.

6 MR. DETERMANN: Just on that last point, I
7 think the CCPA is pretty clear that people could opt
8 out then and then companies can't ask them to opt back
9 in for a year if they made a mistake. When I looked
10 at this hypothetical, I was going to say to my client,
11 you know the discount model you can do without data
12 sharing because the consumers will go and show the
13 discount, and that's how the merchants see that this
14 is in effect and that's how they'll pay you. But the
15 city planners get no more data from you because that
16 would trigger the "do not sell my information" link on
17 the mobile app that causes a lot of hassle.

18 And at the Smart Cities conference in
19 Stanford, the city planners had already complained
20 that they're not getting personal data or any data
21 from the private sector anymore with these privacy
22 laws becoming more and more burdensome on companies
23 who want to share for public purposes because any
24 benefit under the CCPA will count as selling. So even
25 if there was some other leniency or some benefit that

1 the city would offer instead of cash, it's selling, it
2 would trigger the link, and many companies don't want
3 that ugly link on their sites, and they will just stop
4 sharing data. That will be the impact of the CCPA, I
5 think, on this hypothetical.

6 MS. JILLSON: Well, in the interest of time,
7 let's move on to the next hypothetical.

8 MS. ARIAS: Though I think Lothar's
9 statements are actually pretty timely about the "do
10 not sell my personal information" because this hypo is
11 going to cover a little bit of that.

12 All right. So Company C sells fertility
13 trackers in which users can record the dates of sexual
14 activity and diagnosis or treatment for an STD.
15 Company C decides to provide access to de-identify
16 data sets to pharmaceutical companies, public health
17 advocates, and advertisers.

18 Carla Consumer doesn't want her personal
19 information to be sold. Frustrated that she can't
20 find a "do not sell my personal information" link, she
21 deletes the app. A year later, Carla asks Company C
22 to delete all information about her.

23 Tracy, can we talk a little bit about the
24 privacy implications of this scenario?

25 MS. SHAPIRO: Sure. So, you know, first, I

1 would think about the legal framework here and what
2 laws might apply. So, you know, whenever there's
3 health data, my first question is always is there a
4 HIPAA issue? There's no mention to the fertility
5 tracker being a covered entity that gets reimbursed or
6 electronically bills insurance providers. It doesn't
7 sound like it's a service provider to fertility
8 doctors. So there's probably no business associate,
9 BAA, kind of governing the use of the data.

10 But, of course, not being covered by HIPAA
11 doesn't mean that you're not regulated. The FTC, as
12 I'm sure everybody knows, has made clear that they
13 view health data as being sensitive information. And
14 I'm sure they would consider STD and sexual activity-
15 related information to be sensitive. So you've got to
16 think about the implications there with regard to data
17 use and data sharing.

18 I would be thinking about the NAI guidelines
19 that says they're sharing with advertisers, unclear if
20 there's OBA going on, but the NAI speaks to the use of
21 sensitive information, including STD-related
22 information for targeted advertising and the need to
23 get an opt-in.

24 I'd be thinking about CCPA, which doesn't
25 specifically address health information but talks

1 about data sharing and places restrictions there. I
2 think about CalOPPA and transparency requirements and
3 then, of course, GDPR and considering whether you've
4 got a legal basis for processing this data.

5 So with that framework, I think there are a
6 few big issues that jump out at me in the hypo. One,
7 there's the sharing of de-identified data with these
8 three entities. And it sounds like it's a new use of
9 sharing. So it says that Company C decides to do
10 this, which suggests it might be a change in its
11 practices. So with the de-identification, I would be
12 thinking about does this de-identification practice
13 that Company C implements, does it comply with the
14 various standards for de-identification?

15 So with CCPA, we've got a super broad
16 definition of personal information and a really broad
17 and quite circular definition of de-identification.
18 So I think a lot of us are struggling to figure out
19 exactly what -- how one can actually de-identify data
20 at this point under that law. It also requires that
21 one puts in place technical and business processes
22 to prevent the de-identification of data. So we'd
23 need -- Company C would have it look at its contracts
24 that it's got in place with these recipient entities.

25 If Carla's not in California, I'd also be

1 thinking about FTC guidance. On earlier panels, they
2 talked a lot about the de-identification standards
3 that are set forth in the FTC Privacy Report. You'd
4 also need attestations by the recipients that they
5 won't make efforts to re-identify the data. And then
6 if she's in the EU, I would be thinking about GDPR,
7 which also has an incredibly high bar for
8 anonymization, and most likely Company C won't be
9 meeting that standard in disclosing the data.

10 So then we've also got this change in the
11 treatment of data. You know, it is a very basic and
12 long-standing FTC principle that if you have a
13 material change to retroactively collected
14 information, the FTC wants you to get opt-in consent
15 for that. So you'd have to consider here is this a
16 material change in the treatment of information. I'd
17 want to be looking at what Company C told users in the
18 privacy policy with regard to how they share data. It
19 could be that they had a super broad disclosure that
20 would maybe cover this. But if not, they'd want to be
21 thinking about whether they need to get an opt-in
22 consent for that.

23 I think about CalOPPA, which says in your
24 privacy policy you've got to say how you're going to
25 notify your users of material changes, so you'd want

1 to make sure whatever method you set forth there
2 you're complying with that. And then, of course, with
3 GDPR, you'd want to be thinking do you also need to
4 get consent for these disclosures.

5 And then two other considerations. So we've
6 got Carla wanting to opt out. She doesn't want her
7 personal information to be sold, and she's frustrated.
8 So, you know, one, if I were Company C, I'd want to be
9 thinking about if she's a California resident or not.
10 As Rebecca touched on, hard to know how Company C
11 would make that determination at this point. They
12 probably don't have address information. Fertility
13 tracker apps don't tend to collect that kind of
14 information. Can they use IP address? Hard to say.
15 Hopefully we'll get more guidance from the California
16 Attorney General on that.

17 And, then, are they selling information? Is
18 this a sale? So are they -- in exchange for the
19 information, are they getting some valuable
20 consideration? And assuming that it is a sale of
21 personal information, is Carla's deleting the app, is
22 that an opt-out? Is that them directing the business
23 to not sell her information? Under CCPA, they say
24 you've got to have at least two methods, a phone
25 number and a method through the website. So I would

1 say unless Company C said in its privacy policy, if
2 you delete the app, well, that functions as an opt-
3 out, that probably isn't a sufficient opt-out under
4 CCPA

5 Let's see. Lastly, we've got her deletion
6 request. So a year later, she asks the company to
7 delete all information about her. If she's a
8 Californian, she can't ask for all information to be
9 deleted. It's personal information only. So if there
10 is, you know, some kind of an anonymization option,
11 that's something Company C could take advantage of.

12 Similarly, under GDPR, you'd want -- Company
13 C would want to look also to their privacy policy.
14 Sometimes companies, even if they're not legally
15 required to, do make promises in their privacy
16 policies about when they'll delete data. And, then,
17 you'd want to consider whether there are exceptions.
18 So both GDPR and CCPA set out fairly broad exceptions
19 for deletion, so I'd want to consider whether any of
20 those apply.

21 MS. ARIAS: Thank you. That's actually
22 excellent issue spotting. You've covered actually a
23 lot of my follow-up questions, which means you did a
24 great job.

25 But let me -- let me open it up to the rest

1 of the panel. I would love to know if you guys see
2 any other issues that Tracy didn't cover. And let me
3 actually make that question a little bit different and
4 kind of maybe bring a little bit of the last panel in,
5 where Professor Fred Cate said, you know, we should be
6 focusing on the harms. I'm curious if you all see any
7 harms or any privacy implications in this hypo, that
8 maybe are not covered by any of the laws that Tracy
9 covered.

10 Jay, would you like to take a crack at that?

11 MR. EDELSON: Yeah, sure. Yeah, I actually
12 wanted to respond to a lot of what Professor Cate
13 said, so you kind of opened the door. First of all, I
14 think the idea of de-identification is kind of a myth,
15 and so when companies start talking about that, I get
16 skeptical. Years and years ago, before Silicon Valley
17 got really good at figuring out what we do and who we
18 are, Netflix put out a contest to see if people could
19 come up with a better algorithm for picking movies.
20 And they put out -- things seemed totally innocuous.
21 Just no names and just here are some movies.

22 And news reporters were able to actually tie
23 that to specific people. And the level that the
24 really smart companies are able to do that with is
25 shocking. If you have almost any three points of data

1 -- geolocation, for example, but anything even broader
2 than that -- you can find out who somebody is. What's
3 really scary to me is that they're selling this
4 information to pharmaceutical companies who could do
5 whoever we -- you know, whatever we want with it,
6 whatever they want with it.

7 But I want to go back to Professor Cate's
8 kind of preliminary point, which is that we shouldn't
9 worry about consent. And I think he didn't have a
10 chance to fully expound upon this, but it makes some
11 intuitive sense. As consumers, who really reads all
12 these privacy policies? So what does it matter if
13 these companies say, by the way, we're actually going
14 to be tracking all of this stuff and then providing it
15 down the line to somebody else? And the answer is not
16 because the consumers read it, but because others read
17 it.

18 So for example, when Snapchat for a day
19 decided that they weren't going to permanently delete
20 all the snaps, nobody read that in their privacy
21 policy except the blogger, and then it became big
22 news, and Snapchat said, oh, we can't do this anymore.
23 So I think that's the real reason why consent is so
24 important and why companies have to follow that.

25 MS. ARIAS: Lothar?

1 MR. DETERMANN: Just one point. I would
2 say that the pharma companies, of course, developing
3 new cures that would benefit Carla and many other
4 people -- but I'm probably just an optimist on that.
5 And I wanted to add to Tracy's excellent list of issue
6 spotting that we have the California Medical --
7 Confidentiality of Medical Information Act on top of
8 the list that she provided that covers with HIPAA-like
9 rules also providers of hardware, software, and online
10 services since 2015 and requires opt-in consent for
11 certain authorizations.

12 They have to be handwritten -- that's real
13 fun when you have a mobile app. And they have to be
14 signed in a typeface no smaller than 14-point type,
15 although it doesn't specify the font type, only the
16 size of the font. Clearly separate from any other
17 language presented on the same page, executed by a
18 signature that serves no other purpose than to execute
19 the authorization, signed and dated.

20 Plus, we have a separate law that requires
21 consent for the collection of medical information with
22 direct marketing purpose. That's Civil Code 1798.91,
23 I'm cheating here, reading from my own book, making
24 the point that we already have hundreds of laws, and I
25 think we didn't need the California Consumer Privacy

1 Act on top of all of these, unless we repeal some of
2 them or preempt them on a federal level.

3 MS. ARIAS: Yeah, Al.

4 MR. RAUL: So, first, just responding to Jay
5 on the de-identification, you know, if we can't rely
6 on de-identification, we're really cooked in terms of
7 innovation, picking up on what Lothar said. I mean,
8 these public health advocates want this data for a
9 reason, the pharmaceutical companies as well. You
10 know, progress, innovation will stop, and artificial
11 intelligence will be completely developed elsewhere.

12 So if a statute says, like CCPA, that --
13 and, by the way, HIPAA -- says that you can work with
14 de-identified data, we should strive for that. And,
15 of course, de-identified data, if it's been
16 anonymized, isn't even personal information under the
17 GDPR. We could talk for weeks and months and years
18 about pseudonymized data, but I know there are, like,
19 two minutes left, so we won't.

20 A couple of other issues to note. So Carla
21 wants Company C to delete the information about her.
22 It's not clear from the hypo whether the information
23 that remains with Company C is in de-identified
24 format, but if it were, under the CCPA, the company
25 would not have the obligation to re-identify Carla

1 from that in order to find it and delete it.

2 And, then, the request is coming in a year
3 later, so a year later is about 12 months. So the
4 look-back provisions are 12 months for what a company
5 needs to go back. So, you know, maybe depending on
6 when she asks and what remains, you know, the company
7 may not be able to find it, re-identify it, and delete
8 it 12 months later.

9 MR. EDELSON: Can I follow up?

10 MS. ARIAS: Yes, please, Jay.

11 MR. EDELSON: Alan, I'm just curious, in
12 terms of stifling innovation, so let's say you're that
13 company, you come to me and I'm a lawyer, and I say
14 you can do this, you just need to add a sentence
15 saying, by the way, we're going to collect this
16 information and we're going to send it on and we're
17 going to try to make it anonymous and here's how, and
18 that's what we're going to do. You think companies
19 are going to say, oh, it's not worth that?

20 MR. RAUL: Oh, you mean in other words if
21 you make disclosure of the de-identification plan in
22 advance?

23 MR. EDELSON: That's all that's required for
24 most privacy.

25 MR. RAUL: Yeah, no, I think that's right,

1 but I think also we can assume it. When data is
2 collected that it is possible -- I mean, it's
3 contemplated under HIPAA, under CCPA, under GDPR, you
4 know, I'm sure under other regimes as well, that it
5 can and will be de-identified. And, you know, under
6 HIPAA, to be sure, it's perhaps more regulated if the
7 party who is de-identifying it doesn't have full data
8 rights to it.

9 But it's sort of a standard, right? De-
10 identified data is tantamount to anonymized data,
11 really, and people deal with anonymized data all the
12 time. So I don't think it would be hugely burdensome
13 to just say that. You know, we can de-identify your
14 data and then use it for other socially beneficial
15 purposes or commercial purposes, which is, you know,
16 analogous to socially beneficial. Or we could just
17 assume it, that that's what people are going to do
18 with data, that if they can figure out a way
19 effectively to de-identify it within the consistency
20 of the relevant statutory regime, then they're free to
21 work with it because it's to everybody's benefit.

22 MS. ARIAS: So I have a question from the
23 audience, kind of following up on the discussion
24 between Jay and Alan. So given that there's -- my
25 understanding from the audience -- is that the

1 definition in California of the resident is somewhat
2 wide, and, obviously, we have the 12-month look-back
3 period. So the question from the audience is, does
4 the wide resident look-back period essentially create
5 a national right. What are your thoughts on that?

6 MS. SHAPIRO: So in the sense that because
7 you can't -- it's so hard to identify who is a
8 California resident that you will effectively have to
9 give these rights to all Californians. I know of
10 companies that are considering that implementation,
11 that they're looking at what data they have about
12 users and there are some that determine that they
13 don't have sufficient information -- with the guidance
14 that we've gotten so far from the AG's office.
15 Hopefully, there will be something more when we get
16 the regs, but that they might have to just apply this
17 nationwide.

18 MS. ARIAS: Okay.

19 Yes, please, Rebecca.

20 MS. ENGRAV: Two thoughts on, in essence,
21 the de-identification piece. To me, if we think de-
22 identification actually works, you know, if we believe
23 in it, if we decide whatever the standard is -- maybe
24 it's the kind of circular piece way that's defined
25 within the CCPA; maybe it's the existing FTC standard.

1 Maybe we come to something better. But if we believe
2 in that, then there's really no point in, Jay, to your
3 point, notice and consent to people because, like,
4 what are they noticing and what are they consenting to
5 if we believe that, in fact, there's no reasonable
6 chance that they'll be identified?

7 If we don't believe in it, if we think,
8 well, we can do the best we can, but, actually, a
9 really good college student could figure out who you
10 are from this, then I think we need to, all of us,
11 including recipients, including cities and governments
12 that say they're receiving data in de-identified
13 fashion, need to stop telling consumers and kind of
14 over-promising what de-identification means.

15 So I think, like, you can't answer the
16 question, should consumers have a right to either
17 consent and opt-in or opt-out from some sort of de-
18 identified third-party sharing without also coming to
19 a conclusion about what de-identified means, and if we
20 actually think that it still exists as a concept.

21 One other piece to your point --

22 MR. EDELSON: May I just say, I agree with
23 you 100 percent. First time.

24 MS. ENGRAV: That's unusual.

25 MR. EDELSON: Yeah.

1 MS. ENGRAV: There is a way in which even a
2 truly de-identified sharing -- so now let's posit a
3 world in which it's really, really good. Could still,
4 in fact, create some form of personal psychosocial
5 harm to someone. Jay and I probably don't agree on
6 whether that's actionable under a law, but what if the
7 public health advocates or the pharmaceutical
8 companies are also receiving other information about
9 these folks? What if they are receiving the race, the
10 age, the ethnicity, the income status of these users?
11 And what if they are using that as part of how they're
12 formulating whatever their treatment plans or
13 modalities could be?

14 You know, this history is a pretty bad --
15 our country has a bad history in some sectors of
16 making public health decisions about people from
17 different races. And maybe there's a person who uses
18 this app and wants the benefits for themselves but
19 just doesn't want their data to go into that data set,
20 even if it's never going to be associated with them.
21 So that just could be a different -- a way in which
22 even de-identified data sharing could present a risk.

23 MS. JILLSON: These are all great issues
24 that you've all raised, but in the interest of time,
25 we're going to move on to the next hypo. So here we

1 have Company D, which sells smart coffee makers that
2 can be connected to an alarm clock app. The company
3 installs a microphone but does not disclose its
4 presence. Three years later Company D announces a
5 software update that will activate the speaker so that
6 it can respond to commands to make coffee. The
7 company will also data-mine the voice recordings to
8 improve the product.

9 Calvin Consumer is concerned that Company D
10 may have recorded his conversations. He wants to
11 access all data about him.

12 Jay, what are the privacy implications about
13 this scenario, and what can Calvin Consumer and his
14 friends do about it?

15 MR. EDELSON: I think they can do a lot.
16 But, first, I just love this hypothetical because it
17 gets to the heart of the debate about privacy. I
18 always think about my mom when I -- when I evaluate a
19 privacy case. And I ask, would she care about it?
20 And when you look at the hypo, just on its face, her
21 answer would be no. What do I care? I'm probably not
22 going to use the voice-recognition software. If it's
23 in there, there's no harm to me. Jay, you should
24 become a dentist. Why are you wasting your time with
25 this?

1 Here, though, and this was touched on by a
2 previous panel -- this is why it matters so much. So
3 the first thing I would look at as a plaintiff's
4 attorney is I would actually look at biometrics law.
5 Illinois, for example, the Biometric Information
6 Privacy Protection Act, which has become very active
7 over the last couple of years, talks about
8 voiceprints. And what we're seeing is more and more
9 companies -- Google and Amazon, for example, are very
10 good about this -- where they're using people's voices
11 and identifying people by their voices. So you
12 actually help train their systems. They know when I'm
13 talking to Alexa as opposed to my neighbor.

14 The issue with that -- and this was touched
15 on by the last panel -- is that once you're able to
16 connect someone to their voice and you're able to
17 track how they speak, you can find out a ton about
18 them. The example given on the last panel was
19 Parkinson's disease, which seems somewhat intuitive.
20 There are some other examples which are less
21 intuitive.

22 One is research has been able to figure out
23 whether someone is depressed, just by listening to
24 recorded versions of their voice over time. Another
25 thing is there's an Israeli company that claims to be

1 able to come up with personality profiles about people
2 just based on their voice. So they can predict
3 insurance claims, risk of loan defaults, likelihood of
4 employees leaving their jobs.

5 This is all the type of stuff which could
6 result because someone got a coffee maker and wanted
7 to be able to say, you know, I want some coffee. So
8 again, I would look at the biometrics law, Illinois
9 specifically, and I would say, did you get proper
10 consent? Beyond that -- and I know I sound like a
11 broken record -- it always goes back to just general
12 consumer protection statutes.

13 We have a very similar case, and I want to
14 mention to almost all the hypotheticals we have some
15 similar case here. But one that's very similar, we're
16 suing Bose, you know, the high-end headphones. And we
17 allege that they were capturing some information and
18 not telling people. And we sued them under consumer
19 fraud statutes and also wiretap claims. The court
20 accepted the consumer fraud claims, and when it came
21 to damages, something which I would bet some of these
22 people would be skeptical about, they accepted our
23 argument, which is that people are overpaying for a
24 product if they don't understand that that product is
25 secretly spying on them.

1 So when we bring these cases, we bring
2 experts in who do surveys and say, okay, how much
3 would you pay for this nice set of Bose headphones?
4 And someone says -- whatever. I don't know what the
5 price is. I get cheap headphones. But \$400, \$800,
6 whatever it is. Then they say, okay, now they're
7 secretly recording the songs that you're listening to,
8 and how much would you pay for that? And the answer
9 is significantly less. And so those are the types of
10 theories that we would be focused on and that are
11 really starting to pick up steam.

12 MS. JILLSON: Would anyone else like to
13 respond to anything that Jay raised or anything in
14 this hypothetical?

15 MS. SHAPIRO: I would also be thinking about
16 -- it wasn't clear to me from the hypo, are they
17 getting a consent for the software update? Is it an
18 automatic software update that gets pushed out, such
19 that you don't know that the microphone is suddenly
20 recording you? Is there a "wake" word so that it's
21 only recording me when I indicate that it should be
22 recording me, or is it just going to always be on and
23 always recording? And if that's the case, then I
24 would be thinking about ECPA and state wiretap law
25 concerns for recording conversations.

1 MR. DETERMANN: I would just highlight that
2 Jay's mom wouldn't have paid less for this coffee
3 machine because she didn't care, and I think that
4 makes the point on some of this harm argument or
5 speculation here.

6 The other point I would make is that the
7 Computer Fraud Abuse Act already prohibits accessing
8 other people's machines without consent to collect
9 information. That's an old federal law that we
10 already have. And we do have, for example in
11 California, eavesdropping statutes that would capture,
12 if wiretapping doesn't apply. So I think we already
13 have, again to make this point, myriad laws that
14 probably already cover this. And I think the
15 California Consumer Privacy Act was not necessary for
16 this one.

17 MR. EDELSON: Since my mom was invoked, she
18 would -- she would care because if you said you're
19 tracking -- it depends what the implications are. If
20 they're not doing anything with it at all, and they're
21 not storing this information, they're not doing what
22 these Israeli companies are doing or other companies
23 and they're trying to figure out who my mom is and
24 what her social well-being is like, then she probably
25 doesn't care, and there's probably not a very good

1 claim out there for that.

2 But if they're doing all those nasty things,
3 her view would be -- and I know this, because she's my
4 mom -- her view would be I don't want to buy this for
5 any cost. And that's really what we're seeing, that
6 if the companies are misusing the data and not telling
7 people what they're doing with it, most people, they
8 don't say, well, I'll still buy it but for \$20 less.
9 Most people say, you know what, I'll buy different
10 headphones or I'll buy a different coffee maker.

11 MR. RAUL: Is Company D going to, in
12 addition to activating the microphone for voice
13 activation of making coffee, is it going to impose an
14 additional charge on Calvin because all of a sudden,
15 the device has more features? And is it going to
16 impose that charge, you know, surreptitiously without,
17 you know, getting opt-in?

18 And, also, is it going to start a
19 subscription service that will also, you know, poll
20 Calvin -- or Jay's mom -- would you like me to
21 order coffee for you, and then all kinds of other,
22 you know, commercial applications like that? You
23 know, clearly, this is something that shouldn't be
24 done surreptitiously, but if an additional feature is
25 activated by the company, again, one could look at

1 that as progress or getting something for free, if
2 it's disclosed, obviously. But it isn't necessarily
3 all that different from improvements in firmware, or
4 software, that, you know, are just mediated through
5 code rather than having a, you know, a physical
6 speaker and microphone in the device that people
7 didn't know.

8 So would you not want -- you know, again,
9 firmware and software updates that resulted in the
10 possibility being eavesdropped on, yes, that should
11 clearly be disclosed as well. But you could really
12 look on the bright side and say, wow, you know, my
13 product has just improved for free.

14 MS. JILLSON: So let's assume here that the
15 software update that will activate the speakers also
16 brings with it security updates, bug fixes, since
17 updates are often bundled. So if the only way to
18 forgo activation of the speaker is to ignore that
19 whole update and miss out on these bug fixes and
20 security updates, is that problematic?

21 MR. EDELSON: Yes. I agree.

22 MS. JILLSON: And does current law
23 adequately address that situation?

24 And, Alan, you had a very affirmative or
25 strong reaction to that. So how --

1 MR. RAUL: Yeah, no, I mean, it does --
2 that seems -- you know, I don't think -- I'll put
3 myself in your shoes. I don't think the Federal Trade
4 Commission would have a tough time thinking, oh, maybe
5 there's something unfair, deceptive about that. Maybe
6 it was -- you know, and this was a take-it-or-leave-it
7 proposition where there's -- you know, there's an
8 intrusion here, the possibility -- again, there may be
9 other controls on it, that the hypothetical may not
10 fully address in terms of security controls so that
11 there's no chance that there's going to be an
12 inadvertent activation of this without the consumer's
13 knowledge.

14 But, you know, if the idea here is to put
15 the consumer in a position to possibly being exposed
16 to being unintentional to the consumer recorded, you
17 know, then burying it with other security updates, you
18 know, that would seem unfair, and if it's disclosed
19 inconspicuously, potentially deceptive.

20 MS. SHAPIRO: I think the FTC could arguably
21 bring an -- that would be a place where you could
22 actually bring an unfairness case and have a tangible
23 privacy injury, which would be, I paid \$50 for this
24 coffee maker; I was not told it was going to record
25 me; now it records me. I'm assuming that it's not --

1 there's no "wake" word, there's no opt-in, there's no
2 way to turn it off, and I'm now out \$50. Like, that
3 would be a tangible harm.

4 MS. ENGRAV: I think it probably depends,
5 though, exactly what the security risks are that we're
6 talking about that you will not be getting the patch
7 for. I mean, it sounds from the hypo that if you
8 don't install this update the only thing that's really
9 smart about your coffee maker is that it can connect
10 to your alarm clock app. You know, even if that were
11 hacked kind of -- I mean, you know, I don't know,
12 maybe.

13 But it just seems like we need to think
14 through, because if you're not getting that update and
15 you're choosing not to activate the speaker aspect to
16 it, perhaps the risk to you of any -- you know,
17 there's no actual real risk. Like, what's going to
18 happen from --

19 MS. SHAPIRO: Although is the consumer ever
20 in a position to make that judgment?

21 MS. ENGRAV: Right.

22 MS. SHAPIRO: Right? Like, how bad is this
23 big bug?

24 MS. ENGRAV: Well, if we're looking at it
25 under unfairness, then the consumer doesn't have to

1 make that decision. I mean, unfairness isn't about
2 notice or consent anyway. I'm just thinking it might
3 not actually be an unfair situation.

4 MS. SHAPIRO: But does the consumer really
5 have a choice? If they're being told this is a patch
6 to update a bug and they don't know if this bug is
7 catastrophic, they're going to have to install it.
8 And now they've got a machine that's recording it
9 where they didn't consent to it.

10 MS. JILLSON: And should we be taking into
11 account third-party externalities? So if the bug
12 would affect, you know -- gets hacked, it becomes part
13 a botnet, there are external harms.

14 MS. ENGRAV: The botnet of coffee makers?

15 MS. JILLSON: Stranger things have happened
16 in IOT, but in the interest of time, we can move on.

17 MS. ARIS: Yeah, so let's move on to the
18 last hypo of the day. Company E offers a free
19 internet browser to consumers. It mines browsing
20 history and behavior to infer demographic information
21 about consumers, which it sells to advertisers. It
22 turns out that one popular data set is for females 10
23 to 12 years old. Candace Consumer, not Jay's mom,
24 requests access to all data Company E stores about her
25 so that she can correct any inaccurate data.

1 Alan, last but not least, you want to walk
2 us through the privacy implications?

3 MR. RAUL: Thanks, Andy, and, you know, I
4 don't know that it's really fair to have had a
5 hypothetical about coffee, you know, at 4:45 in the
6 afternoon, you know, just as everybody is starting to
7 doze off to hear me address this hypothetical.

8 But, you know, today is a very exciting day,
9 I think, in our field, and I'm going to explain.
10 Maybe it was already talked about. But, you know,
11 normally, as some of you know, you know, I talk about
12 -- because you've asked us, Elise, and you, Andy,
13 asked us to speak as everyone else has about the way
14 different platforms might approach these
15 hypotheticals. So, you know, normally, that would
16 involve a recitation of the US leadership on privacy
17 going back to 1791 and the Bill of Rights and the
18 right to be let alone in 1890 and the FTC Act in 1914
19 and the Privacy Act, which embodied the fair
20 information practice principles in 1974, Gramm-Leach-
21 Bliley in 1999.

22 But today -- yesterday, in the UK -- and I
23 don't know if anybody else has addressed this -- but
24 there was a -- the UK Government announced an online
25 harms white paper that is going to lead, according to

1 the UK, to new regulation with strict new enforcement.
2 And I really commend this to everyone's attention.
3 And it may turn out to be relevant to this
4 hypothetical, which is about 10 to 12-years-old kids.
5 And that is it's about online harms. And I know that
6 Professor Cate addressed this, Lothar did earlier, and
7 there has been a lot of discussion about harms.

8 When one goes to privacy discussions,
9 frequently we're talking about regulations and
10 procedural and administrative hurdles and not so much
11 the bad things that can happen as a result of privacy
12 infringements. Well, the UK in this white paper
13 yesterday, it's 102 pages long. It has charts and a
14 litany of real harms.

15 Now, it does purport to not cover privacy
16 and data protection, which is the mandate of the
17 Information Commissioner's Office, or hacking, but the
18 fact is, it really addresses everything that we're
19 worried about online for concerns about children --
20 exploitation, sexual abuse, addiction to the internet,
21 access to inappropriate content -- real harms.

22 And so I really do say that this is a
23 development, I think, that we should all be thinking
24 about in future regulation. We know that in the NTIA
25 request for comments that the Commerce Department

1 issued, it also focused on harms. So I think that as
2 we consider these hypotheticals and, you know,
3 especially this one, which is about, you know, dangers
4 online to children, so the first -- turning not to the
5 broad focus on the right approach, philosophical
6 approach to privacy regulation, so question -- this,
7 obviously, since it's 10 to 12 years old, it raises
8 the question of whether COPPA would apply.

9 And so the first question is does it really
10 cover -- does COPPA apply here? This is an internet
11 browser. So COPPA applies to operators of websites
12 and online services. Clearly, is a browser in this
13 context such a website operator or online service?
14 You know, ISPs are not considered, as the FTC has
15 stated, to be covered. Are browsers? Is it analogous
16 to, perhaps, a plug-in or an ad network in this
17 context? You know, so I think that's an issue.

18 Just some other basic questions. Does the
19 browser have to provide a privacy policy under COPPA?
20 If it applies a privacy policy under CalOPPA, if it's
21 collecting information about California residents? So
22 is this browser in some way directed to children? You
23 know, even though the popular data set concerns
24 females 10 to 12 years old, there's no indication as
25 to whether they -- they know that the children are --

1 you know, that the people that they're tracking are 10
2 to 12 years old, or that the service is in any way
3 directed to 12 years old.

4 Is there a persistent identifier involved
5 that would be a potential trigger under the Federal
6 Trade Commission's regulation, under COPPA, or what is
7 the basis for tracking so that it would invoke COPPA?
8 Passive tracking, if that's what's going on, would be
9 certainly within the scope of COPPA, and as well, the
10 CCPA. And, then, questions of access rights, how do
11 you -- in a prior version of the hypothetical, we
12 didn't say who the -- whether it was Candace
13 Consumer's relationship -- and I guess it's not here,
14 either -- whether this is -- what is the relationship
15 of Candace to anyone in the data set of 10 to 12 years
16 old?

17 Is the company going to be able to find data
18 or to -- under CCPA they wouldn't be obligated to re-
19 identify data. Under COPPA, is the data -- if it is
20 attributed to a persistent identifier, is this
21 something that is pseudonymized or de-identified. Is
22 re-identification going to be possible? And is it
23 going to be required? Is there a right to
24 rectification of the data, to correction of inaccurate
25 data?

1 Under COPPA, there's access by the parent to
2 the data about the children if they can be verified,
3 but not necessarily to correct inaccurate data. Under
4 the GDPR, there might be such a right under CCPA,
5 likely not a correction right, although, certainly, an
6 access and a deletion right.

7 Thinking about other parties' obligations
8 here, is there an obligation of the advertisers who
9 are receiving this data? Do they have knowledge? I
10 mean, are there websites where they're -- this is
11 analogous to a plug-in perhaps, where the website has
12 invited this browser in and is somehow responsible for
13 the information that the browser is collecting on
14 behalf of the websites?

15 And, then, are there obligations on the
16 part of the browser company to provide other COPPA
17 requirements for protecting the security,
18 confidentiality, integrity of the personal information
19 of children, if it's -- you know, if it's not de-
20 identified? So we have some age issues here under
21 COPPA. This data set for females 10 to 12 would be
22 covered as under 13. Under the GDPR, the consent age
23 is -- consenting to processing as specified in the
24 GDPR is 16, but member states in the EU can lower that
25 to as low as 13.

1 Under the CCPA, we have two standards for
2 age, as everyone has heard a lot about: under 13 for
3 opt-in by the parent or legal guardian; under 16 for
4 affirmative consent to sell data from the child
5 itself. The tracking and profiling would raise
6 heightened concerns, heightened requirements under
7 COPPA and GDPR. I've talked about the persistent
8 identifier and is this really capable of identifying
9 Candace or anyone else in the data set?

10 Under -- you know, under COPPA, would COPPA
11 apply at all -- again, because with regard to the
12 deletion right, COPPA applies to data that's received
13 from the children. The CCPA also applies to the
14 deletion right, applies to data that is received from
15 the subject, not anything about the subject. There's
16 some ambiguity in that, although the statutory text
17 certainly suggests that deletion of data received from
18 children is the way the CCPA works. The GDPR, on the
19 other hand, concerns any data about any individual.

20 So the authentication issues here will be
21 significant. How does Candace Consumer or her parent
22 verify that they have a right to correct this data or
23 access this data? And I think those are the issues
24 that I would flag.

25 MS. ARIS: Great, thank you. And those are

1 great.

2 So I'm going to open it up on the panel, and
3 I'll give you a choice. You can either react to the
4 hypo, or since we are nearing the very end of our
5 panel, you can either give your closing thoughts maybe
6 on some of the current laws and the applicability and
7 maybe some of the gaps in the current laws as they
8 stand as they relate to privacy.

9 Lothar, do you want to start?

10 MR. DETERMANN: I'll do the reaction to the
11 panel, and Alan made a great analysis already. I'd
12 observe this: The California Consumer Privacy Act
13 would require parental consent or opt-in consent from
14 16-year-olds, and that will lead like COPPA has
15 already that people are excluded from websites. I
16 think that's the main repercussion of this. Children
17 are excluded. Every website policy says you have to
18 be 13. In the future, it will be 16. And that is the
19 main achievement here.

20 None of our hypotheticals actually delivered
21 any harm to us. Did you notice this? We have here
22 that demographic data is sold but not what could
23 happen to the children? We heard that on other
24 panels, that is there, and I don't want to diminish
25 it. But I would say we have to act against those

1 harms. If somebody is exploiting the children, let's
2 do something about exploitation of children but not
3 necessarily about collecting information about them.

4 If in the fourth hypothetical, the coffee
5 machine could be turned on and create voiceprints and
6 they're being abused for something, let's prohibit
7 that but not necessarily prevent coffee machines from
8 reacting to voice commands instead of pressing a
9 button.

10 And I could go to the other ones. The
11 pharmaceutical development, the public health -- none
12 of these delivered harm, and, yet, the CCPA, the GDPR
13 pretty much prohibit everything that is being done.
14 And I think that is symptomatic to many of our
15 hypotheticals and something we should all think about
16 as we're exploring new approaches to privacy.

17 MS. ARIAS: Jay, any thoughts?

18 MR. EDELSON: Yeah, and I'm glad for that
19 lead-in because I wanted to talk about harm, too. I
20 think this is the great philosophical debate about
21 privacy, which is do we adopt the model where we have
22 to wait until something really, really bad happens,
23 and then someone can sue or do something about it?

24 And, I mean, it's an awful example, but the
25 idea of child exploitation, that we know that a

1 dangerous situation is being created, but we've got to
2 wait, and then when that happens, that child can
3 somehow bring suit and recover damages as if that's
4 going to be terribly helpful.

5 The best analogy for this is in the data
6 breach context. And I think the FTC has really taken
7 a lead, where they have brought data security
8 lawsuits, where they've seen that companies have
9 vulnerabilities, and they recognize that there may be
10 a hacking that could happen, and once there's a data
11 breach, the idea that you can make people whole is
12 just not true. It disrupts people's lives. There's
13 identity theft and all of that. It's just not worth
14 it to them to go to court and try to get some amount
15 of money back. What they really want is to avoid the
16 data breach in the first place.

17 And so the FTC, as leaders in this, have
18 started bringing -- or for actually many years -- have
19 brought suit and have said, you know, when you have
20 vulnerabilities out there -- and often they've matched
21 it to what the public-facing statements are -- so we
22 protect your privacy, and have fallen short on that,
23 they go in and say that's consumer fraud and you got
24 to fix those vulnerabilities.

25 And I think that's really where privacy laws

1 should be focused on, how do we prevent the really bad
2 harms before they happen as opposed to just wait for
3 it and then try to fix it.

4 MS. ENGRAV: I'll just respond to one of
5 those points a little bit. I think that taking the
6 data breach example and the FTC bringing enforcement
7 actions, what that hasn't solved for, though, is there
8 are undoubtedly other companies out there right now
9 with the exact same vulnerabilities, and they aren't
10 sophisticated enough to even know they've been hacked.

11 So if what we want to do is decrease the
12 risk of that even happening, we're going to have to
13 find a way to move beyond case-by-case enforcement
14 after there's a big issue, because right now, it's not
15 a level playing field. The companies that are
16 investing huge amounts of money in data security and
17 doing a really great job of it, maybe because they've
18 already had an enforcement action, maybe just because
19 of their size.

20 The other, you know, companies, you know,
21 all those great mom-and-pops, all the wonderful small
22 startups that we hope develop and bring the wonders of
23 the digital economy to all the small communities in
24 America, they're not doing any of those things. So if
25 we think that there are data security steps that are

1 fundamental to even doing an online business, we have
2 to find a way to communicate them in actionable ways
3 and not just rely on case-by-case enforcement.

4 MR. RAUL: I agree with Jay. We shouldn't
5 wait until it's too late to protect consumers and
6 citizens from harms, but I think it's incumbent upon
7 policymakers and the interested public to try to
8 identify those harms, act only insofar as -- or
9 balance, you know, do a cost-benefit analysis to
10 protect the public against those harms, but not
11 stifle, you know, innovation and economic opportunity
12 and so on.

13 And if we aren't smart enough to think in
14 advance about the harms we want to protect the public
15 from, we've got the backstop of Section 5 of the FTC
16 Act and the state UDAP statutes, you know, to
17 prosecute unfair and deceptive acts and practices.

18 What I -- you know, I commended the
19 audience's attention to the UK online harms white
20 paper, which really chronicles so many different harms
21 that are really -- you know, online manipulation,
22 disinformation, you know, exploitation, and attacks on
23 children -- that it's a great place to start.

24 Another place to go to as well is the Spokeo
25 decision in the Supreme Court, where the Court, while

1 not finding standing in that case, that is to say
2 concrete injury for an alleged violation, the Fair
3 Credit Reporting Act, the Court did say that
4 intangible injury can be real and can be actionable,
5 but it's got to be grounded in some recognized either
6 statutory principle where Congress or another
7 legislature has identified a harm, or in the common
8 law or in the long tradition that we have of
9 protecting people against highly offensive invasions
10 of privacy.

11 So I think we -- you know, we can look to
12 those models, and this is also in the request for
13 comments of the NTIA -- to come up with a new
14 framework. And you can also look, by the way, if you
15 read all of the GDPR, as I did recently in order to
16 address the question of what does the GDPR say about
17 harms, and the answer is that most generally, it
18 speaks about just abstract infringements of
19 fundamental rights and freedoms. And these are
20 important fundamental rights and freedoms, but was
21 there anything concrete in there? And it's data
22 security -- Jay's point -- you know, data security,
23 which I think we can all agree that's important.

24 And then it gives concrete examples of where
25 potentially profiling, and the FTC wrote a great

1 report on, you know, big data inclusion or exclusion,
2 but where profiling could lead to actual, tangible
3 impacts of being denied credit, being denied
4 insurance, being denied employment, being denied other
5 opportunities. So, you know, even the GDPR and the EU
6 knows how to frame real harms, and, of course, which
7 is what the US tried to be in Gramm-Leach-Bliley for
8 financial harms, HIPAA for healthcare harms,
9 Electronic Communications Privacy Act for electronic
10 harms, video privacy, you know, educational privacy,
11 et cetera.

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 CLOSING REMARKS

2 MR. TRILLING: I apologize for being in the
3 position of cutting off our discussion. On behalf of
4 the Federal Trade Commission, I just want to take a
5 few seconds to thank all of our panelists and speakers
6 for sharing their insights and providing us with an
7 outstanding discussion today. I also want to thank
8 our audience and our online audience.

9 We look forward to another interesting day
10 tomorrow when we'll be discussing the role of notice
11 and choice, the role of access, deletion, and
12 correction. Then we'll have remarks from Commissioner
13 Rebecca Kelly Slaughter. And after lunch, we'll
14 conclude the hearing with a panel on accountability,
15 and a two-part panel discussion on the adequacy of the
16 FTC's toolkit for protecting consumers' privacy.

17 With that, we will resume the hearing
18 tomorrow at 9:00 in the morning.

19 (Applause.)

20 (At 5:07 p.m., the hearing was adjourned.)

21

22

23

24

25

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

CERTIFICATE OF REPORTER

I, Linda Metcalf, do hereby certify that the foregoing proceedings were digitally recorded by me and reduced to typewriting under my supervision; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were transcribed; that I am not a relative or employee of any attorney or counsel employed by the parties hereto, not financially or otherwise interested in the outcome in the action.

s/Linda Metcalf
LINDA METCALF, CER
Court Reporter