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
MR. TRILLING: Good morning, everyone.

Welcome to the Federal Trade Commission and the first day of our hearing on the FTC’s Approach to Consumer Privacy. My name is Jim Trilling. I am an attorney in the FTC’s Division of Privacy and Identity Protection. Before we get started with the substance of the hearing, I have a number of brief administrative announcements that will apply throughout the hearing.

First, if you leave the Constitution Center building during the hearing, you will need to go back through security screening again, so please allocate time for that.

Restrooms are located outside of the auditorium, in the hallway, and the Constitution Center building cafeteria is located around the corner on this floor of the building. If an emergency requires you to leave the auditorium but remain in the building, please follow the instructions that will be provided over the building’s PA system.

If an emergency requires evacuation of the building, an alarm will sound. Please leave the
building in an orderly manner through the 7th Street exit. When you get outside, turn left and proceed
down 7th Street and across E Street to the FTC emergency assembly area and remain in that area for
instructions to return to the building or otherwise. If you notice any suspicious activity, please alert
the building security staff.

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

The webcast recording and transcripts of the hearing will be available on the FTC’s website shortly after the hearing concludes. Webcast recordings and transcripts from all of the FTC hearings on competition and consumer protection are available on the FTC website. Audio files from the hearings are available to be streamed or downloaded at FTC.gov/audio.

Please silence your cell phones and other devices. We want to make sure that everybody has the ability to be heard. Attempts to address the hearing speakers while this hearing is in progress and other
actions that interfere or attempt to interfere with
the conduct of this hearing or the audience’s ability
to observe the hearing are not permitted. Any persons
engaging in such behavior will be asked to leave.
Anyone who refuses to leave voluntarily will be
escorted from the building.
During the panels, the audience is invited
to submit questions via question cards available
from FTC staff and in the hallway outside the
auditorium. If you would like to submit a question,
please write the question on a card and raise your
hand to signal for FTC staff to collect the question
from you.

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

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

With those logistics out of the way, we can
now move on to the substance of the hearing. I am pleased to turn the podium over to FTC Chairman Joseph Simons for opening remarks.

(Appause.)
OPENING REMARKS

CHAIRMAN SIMONS: Well, good morning, everyone, and welcome to our two-day hearing on the FTC’s Approach to Consumer Privacy. We are so excited for this event. Over the past two years, we have seen technology develop that was nearly unimaginable only a few decades ago. Tiny computers sit in our pockets and funnel news, messages, and more our way. Smart speakers do our bidding. Other smart devices unlock our doors, set our thermostats, and turn out the lights. Robots powered by artificial intelligence are becoming commonplace on factory floors, and self-driving cars are on the streets of Pittsburgh, Boston, Las Vegas, and San Francisco.

What unifies these remarkable inventions is what fuels them -- data. We live in an age of truly amazing technological changes powered by data, but along with enormous benefits of data-driven innovations comes a certain degree of risk. News stories highlight troubling privacy practices on a regular basis, whether it’s allegations of surreptitious recording by internet-of-things devices, inadvertent exposure of health information, or the sharing of personal data beyond consumers’ authorization.
Have we become inured to these privacy incidents? Not at all. In the face of these disclosures, consumers report that they do care about their privacy and that they value the ability to control what information is collected about them and who can get that data. These concerns arise from the recognition that privacy violations can cause a range of real harms, including fraudulent charges on credit cards, safety risks, reputational injury, and unwanted intrusion into people’s homes and the intimate details of their lives.

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

The FTC has long been the cop on this particular beat. Over the past two decades, we’ve brought hundreds of cases, conducted over 70 workshops, and issued about 50 reports to help protect consumers’ privacy. Our work over the last year...
demonstrates the FTC’s approach to consumer privacy, vigorous enforcement with every tool that we have. For example, in February, we announced a settlement that includes the largest civil penalty the Commission has ever obtained under COPPA. Last fall, we obtained a $3 million civil penalty under FCRA against a company whose automated decision-making tool provided inaccurate data to property managers, resulting in denial of housing.

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

We’ve also filed two advocacy comments, announced five public events, issued a staff report on privacy injuries, and issued a notice of proposed rulemaking to help military personnel get free credit reports. As this list of accomplishments demonstrates, the FTC has done a remarkable job to protect consumers’ privacy with the tools and the resources at our disposal. But we must do more. We
need to continue evaluating privacy risks as they evolve. What approach will protect consumers’ privacy interests while fostering innovation and competition that has brought us so many benefits?

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

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

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

And we will round out today’s session with a
two-part discussion about current approaches to privacy. Panelists will discuss, compare, and contrast US and international privacy laws and self-regulatory frameworks. As policymakers consider privacy legislation, the panelists will consider what such a law might look like.

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

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

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

Finally, two sets of panelists will discuss
whether the FTC has an adequate toolkit for protecting consumer privacy, covering topics such as the use of our existing authorities, as well as the need for new resources.

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

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

(Applause.)
GOALS OF PRIVACY PROTECTION

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

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

Next to Neil is Alastair Mactaggart. Alastair is the Chairman of Californians for Consumer Privacy, and you all probably know him best for his leading role in the passage of California Bill 375, better known as the California Consumer Privacy Act. And, finally, next to Alastair is Paul Ohm.
Paul is Professor of Law and the Associate Dean for Academic Affairs at Georgetown University Law Center. Paul is a leading scholar in information privacy, computer crime, intellectual property. All things digital really, that’s Paul. And, also, he did a stint here at the FTC a few years ago as a senior policy advisor working on these very issues.

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

So when we think about, really, any regulation, any type of government intervention, we should ask a couple of questions. The first is what do consumers want. What is it that -- what are their demands? The second thing, and I’m saying this as an economist -- and I’m putting my economist hat on -- the second thing that we should be interested in is, well, if there’s something that consumers want, if there’s a market, if there’s some transaction that should be occurring, is it happening, is the market
able to mediate these demands, often referred to as a market failure? And that’s bad for society. If there’s a market failure, that means that there is some kind of welfare-increasing transaction that is not occurring.

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

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

But we also see revealed preference, which
is when actual trades are made in the marketplace, when actual decisions are made, that there is a lot of evidence, both experimental and in the real world, to suggest that, well, consumers are willing to trade information about themselves for a very small amount. This has given rise -- this is what is referred to in the privacy literature as the privacy paradox, and it’s something, at least in the academic world, that we try to square. It is a paradox. Why do we see on one hand that privacy is clearly something that people care deeply about, but, in the real world, they seem to make different trades?

So the next question is, is there some kind of market failure? Are consumers really getting the type of privacy protections that they want? So we said that revealed preference suggests that the consumers are willing to trade information for small amounts of money or convenience or access to content. Well, what revealed preference will -- a market outcome will correctly show consumer preferences, but markets don’t always work. There could be failures like asymmetric information. The data ecosystem is notoriously complex, do consumers really understand what’s going on? Behind the scene, there are also cognitive biases.
Alessandro Acquisti and a lot of his colleagues at Carnegie Mellon have done a lot of work in this area, but we all know that consumers from the behavioral economics literature suffer a variety of systematic errors, especially in being able to assess long-term benefits and cost. So we have those -- we look at that.

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

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

We also know that there is a powerful
incentive for firms to reveal good things about them relative to their competitors. It’s this unraveling principle that if I can credibly show you that I, say, provide more privacy than my competing firms, then I have a really, really strong incentive to do that because I’ll gather more customers.

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

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

So if the market isn’t mediating the demand for control over information, well, government intervention can provide that and increase welfare.
At the same time, there are costs -- there’s a large literature, both empirical and theoretical, that retarding information flows can have negative impacts on market performance and innovation, and we’ll talk in a second about some of the research that was presented back in the fall at the hearings. And, finally, when we think about what government should do, the form of intervention matters. Do we want to have an enforcement regime where we go after identifiable harms with law enforcement, take people to court, kind of in the way that the FTC acts now? There’s ex ante regulation in the sense of commanding ahead of time what firms need to do. There’s the FIPPs model. There are lots of different regulatory models, and so the form that it takes really can have an impact on government intervention.

So taking that framework and now moving -- I want to go back to the fall and think of this as maybe the last episode of the FTC privacy hearings, just as a recap to bring you up to date, to inform some of these questions that we need to think about when we think about the goals of privacy protection. So what have we heard? We heard, again, going to privacy paradox that even with full information we
have experimental evidence showing that consumers choose to reveal private information for very little compensation.

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

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

We think about the costs and often privacy regulation. We think of opt-in versus opt-out. One of the big areas of potential costs is the revenue
generated from targeted advertising. So what do we find? Well, a lot of research, we had a lot of experts at that hearing, a lot of people who are expert on the online advertising ecosystem, and we heard that behavioral targeting tends to generate more revenue for content providers than contextual advertising. There seems to be a lot of empirical evidence to suggest that, but there needs to be some caution.

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

We saw that there is increased revenue to content providers from targeting, but it tends to be larger than the correctly measured lift to advertisers. Again, it goes to maybe this difficulty in measuring lift. We also heard interesting work
from Catherine Tucker that suggested despite the idea
that AI and big data algorithms know everything about
us and are able to predict with just scary accuracy
that, in fact, she unpacked some of these algorithms
and found that they weren’t -- they were worse than
chance at predicting gender, for instance, that there
are a lot of -- that maybe the targeting and maybe the
fears of AI, the privacy fears aren’t that much. And,
also, the flip side of that is the extent to which
opt-in versus opt-out is going to have a big impact on
revenue, maybe we need to investigate that more
carefully.

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

Finally, again, more evidence from Liad
Wagman, as well as Ginger Jin, Former Director of the
Bureau of Economics, saw that looking at the impact of
GDPR on VC investments, some interesting -- at least this is early-phase research and looking at the short run, is that there was a negative impact, somewhere between 27 and 56 percent in value, for European startups versus their counterparts in the US using good treatment and control methods. We also heard about work from Catherine Tucker and Amalia Miller about the negative impact in HIT investments and on health outcomes.

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

There is also the notion that bigger firms are more able to deal with regulation than smaller firms. However, these results are sensitive both to consumer preferences for privacy and on market structure, elasticity of demand parameters in the model. And, again, it’s theoretical work. We don’t really -- we didn’t really have any empirical work on that.
So with bringing us up to date in setting the stage, I’m going to sit down here and begin a discussion with our esteemed panel to drill down on some of these issues as we think about the path forward in protecting -- our goals in protecting privacy protection.

All right.

MR. CHILSON: Thanks, James.

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

(Laughter.)

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

MR. CHILSON: Well, I think the first step to answering that question, I’m going to take it back a little bit further, and I think the first step is to define what we mean by privacy, and it’s a very
complex word. There’s a lot of values that people put into the word "privacy." I’ve been on panels where the discussion has ranged from identity fraud, you know, concerns about identity fraud all the way to misinformation and election manipulation. Those are radically different problems.

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

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

And so information is the content of a
signal that’s going from one party to another. So, for example, the sounds that are coming out of my mouth contain information, they carry information. The light that’s reflecting off my body contains information. And because we exist in the physical world and we interact with the physical world, we’re constantly generating information, and we can’t control -- we can’t control all of it. We can try to control certain things and, in the physical world, we understand what the limits of that control are.

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

If my goal is to constrain information, it immediately demonstrates that there’s two parties involved. There’s me and then the party who is presumably going to collect or use the information, probably many other parties as well, and my privacy protections are in tension with that person’s use of information about the world, and that we have to draw
lines somehow about how we’re going to divvy up someone else’s ability to observe the world and use that information, sometimes to serve me, sometimes to serve their own purposes, it depends, and my rights -- my control, my physical ability, but then also my interests in controlling information.

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

MR. COOPER: Finally.

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

Now, if you get further out from that, there can be disagreements around what other types. And the
Chairman mentioned a bunch of different types of harms and some work that Maureen Ohlhausen did in talking about informational injuries, also talked about this. And the types of harms that the FTC has looked at are not just financial harms, are not just, you know, these safety risks or safety injuries, but there are some other harms that are often mentioned in FTC cases. We do have reputational harm. We do have invasion of the home. Now, reputational harm in FTC cases has never been a sole vector for a case, but it is one thing that the FTC has recognized as a potential injury.

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

And the reason I think that government intervention is best justified the closer you get to
that core is because government’s resources are limited, and, so, if we are focusing on less tangible and more -- less objective injuries, and to the cost of focusing on objective, concrete injuries to consumers, we’re probably, on balance, leaving consumers worse off. So if we’re ignoring some actual harms that we know about, some ones that everybody agrees on, and we’re doing other things, we might be making consumers worse off.

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

Tangible objective injuries are easier to redress. When we’re talking about financial harm and we can put dollar amounts and compensation around physical injury, you can’t make somebody perfectly whole, but we have models in the past through tort law that show how we might approach those problems. Other
types of injury, it might be harder for government to
work on.

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

And so we need to be very careful on that,
and that happens less and less the closer you get to
that core of physical or financial injury. That’s not
to say that there aren’t other issues that government
should play a role in, and it can play a lot of
different roles, but we have other tools other than
government intervention, and I think a lot of the
other panels will talk about that, but that’s sort of
how I think about harm as the core harms and then as
sort of concentric circles that build out from those.
And we’re safest with government intervention in the
center, and we’re taking more chances that we’re
drawing the lines wrong and potentially making consumers worse off the further out we get from that center.

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

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

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

And I think if our role as first panelists to is exhort the FTC, which has been a phenomenal leader in this space but is at a crossroads where
increasingly politicians, people with power, and average citizens seem like everything is going to hell in a handbasket, to use the technical phrase, online, I think it’s really incumbent on the FTC to think hard. And I’m glad to see so many of my former colleagues on the staff, about what that means for this agency.

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

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

And, again, in a 2012 context, that’s an important list and it’s a list that the FTC still has
to put at the center of its work. They talked even about harms to intimacy and dignity, and the FTC has brought cases around that. But I think to talk about this in a 2019 frame, you really, really do have to update the kind of harms that not only the world seems worried about but this agency seems well positioned to address. Manipulation is something we weren't thinking about much in the 2012 context but definitely should gather new light.

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

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

Okay. So I will take two minutes to talk
about the privacy paradox, though I have about 14
minutes’ worth of things to say about it, and then
I’ll invite you to ask me another question and I will
continue my answer.

(Laughter.)

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

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

MR. OHM: Yeah, yeah, yeah. No, that’s
right. And I warned you in email that that’s my
shtick.

MR. COOPER: He was pretty --

MR. OHM: I was pretty transparent that
that’s what I do. And I’ll do this within a privacy
-- an economist framework, right, in terms of kind of
behavioral economics and in terms of the kind of
cognitive manipulation that happens around choice and
consent. It’s crazy to think that any of the
preferences that we’re measuring in any of these
"studies" are revealed. They’re manipulated, they’re bought, they’re controlled.

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

Okay. I’ve taken too much time. Thank you.

MR. COOPER: All right, thank you.

Alastair, do you want to jump in?

MR. MACTAGGART: Sure, I would. I think one of the problems that, the way I see it, is that we’re trying to address the situation where just by living in the world, your entire life is being tracked and manipulated. So when I think about privacy, I think about different stories. So in 2017, the
Massachusetts AG settled with Copley Advertising case. They were waiting until women were inside reproductive health centers and then sending them right-to-life chats, saying that’s a child, not a choice, right now, don’t do it.

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

Cars are essentially data-gathering, you know, machines on wheels, and they know how often you eat at a fast food restaurant, how often you go to the gym, and how long you stay there, and what time you get to work and when you leave and whether you’ve been fired before anybody else knows whether you’ve been fired. So we have to live our lives. The technology is interwoven into our lives, and we really don’t have any choice.
And I think the harm we’re trying to address is how we do start to get some kind of balance back just by living our lives. And, yes, at some level you could say, well, this is all voluntary, you know, you get to use this technology, you choose to use it, but you’re sort of -- your choice that you’re left with is to go kind of live in the stone ages and not really be part of the modern world.

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

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

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

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

MR. COOPER: Neil, I know that Paul took on
a few things you said, so I want to give you a chance
to respond.
MR. CHILSON: Sure. So, you know, I think all of these are old ideas, Paul, to be fair. And, in fact, the idea that our technology is manipulating us is as old as technology is. You can follow pessimist archives on Twitter and you’ll see just tons of stories, or listen to their podcasts about how TV, advertising, novels, comic books, speech -- writing was a technology that was ruining society by manipulating people in ways that they could not control.

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

And, so, Alastair, I think you made a great point that we live in this amazing technological environment where a lot of the problems that we’ve been trying to solve in our lives are now adaptable to being solved through software. And the key to that is information, and in order to get those benefits, we need to maximize the ways that we can share that information, and we also need to respect that information is -- information that involves us is not purely about us.
And so my interactions with somebody’s computer out there on the internet -- I think sometimes we have this perception that I’m sitting in my living room, I’m browsing the internet, and so the internet’s, like, on my computer. That perception is not any more correct than if I wandered out into the streets naked and then said, nobody is allowed to look at me. We don’t have rules that say that.

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

Sometimes that can make sense when there are certain types of harms, but, again, that’s at the core set of harms, not the -- and I don’t think we need to perpetuate the idea that we have somehow more control than actually is feasible or possible to achieve while gaining the benefits of that technology at the same
MR. COOPER: Thanks, Neil.

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

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

MR. OHM: So property rights are not the right way to think about it. So this isn’t about, you know, can we convince people to take $1.25 and then we can market any way they want. Implicit in the question and I think implicit in the kind of core foundational argument -- and explicit, it was in one of your slides -- is that, when we have something like meaningful and restrained privacy law, we’re going to kill the internet as we know it. So let just me riff
on that for a second.
So I think both the empirical evidence that you had on your slide, but I think, more broadly speaking, is not nearly as strong as is represented. And, in fact, it’s always curious to me that the demands for rigor only flow in one direction in this debate, which is we need, you know, more proof that these harms are real harms. They don’t feel like real harms, and yet we don’t cast the same skeptical eye on claims that if we, you know, have CCPA or if we have GDPR this is the end of society as we know it.

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

And I think one of your slides said, well, now we know, it’s been proven. It has not been proven. There is a thin read of evidence it’s a little thicker than it was back when I was at the FTC.
The only people who can do these studies are the people who can get the data from the ad companies. One of the kind of noteworthy studies in 2013 was by a Harvard Business School professor who refused to put it in his scholarship part of his CV; he put it in his paid research part of his CV. And remember, we’re talking about contextual advertising which fueled the massive growth of the internet up until about 2007. Sure, there was some behavioral at the time, but companies like Google hadn’t yet flipped that particular switch.

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

And so the question is what if -- what if -- we could wave a wand and we could say no more kind of third-party tracking just for behavioral advertising purposes? You know what my guess is? We’d have tons of innovation and tons of money, and what’s really exciting is the innovators would not be focusing on, you know, to quote a famous Facebook engineer’s quote,
the best minds of my generation are trying to get
people to click on ads. They’d be focused on
meaningful content and making a connection with their
users and building a community and improving society.

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

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

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

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

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

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

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

You know, as Paul said, the technology that
fueled the creation of Facebook and Google, contextual
advertising, no one really finds that very offensive.
It’s the sense of being tracked and who you are being
anticipated before you even know it, that’s this kind
of weird technology that I think people really are
objecting to. And in terms of harms, I couldn’t agree
with Paul more, everybody always talks about the
harms. My question is harms to who. It’s not a harms
to the consumer. It’s the harms to market cap of
Facebook and some of these other firms, you know, and
I think the last time you ever heard, you know, a
consumer saying, you know, my problem with that site
is I just don’t get enough behavioral targeted ads. I
mean, who’s ever said that, you know?

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

But the reason that all these people -- all
the companies are waving their hands panicked about
choice is they know that if consumers have effective
choice that’s easy to implement, they will take it,
and that’s why everybody is fighting to try to stop
that from happening, because they’re making so much
money selling your information. And people are tired
of their information that they’re generating just by
living their lives being sold and themselves being the
market -- being the product.

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

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

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

And, so, when you say that it’s just about
choice, it’s not just about choice. It’s about the
frameworks in which consumers make choices. And when
those choices are one size for all the certain
problems, and when consumers have widely ranging
privacy preferences, different choice frameworks are
better for certain consumers than others. And so if
we’re going to just say here’s the one single choice
framework that everybody has to do, we’re going to be
benefitting some consumers, absolutely, without a
doubt, and we’re going to be harming others.

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

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

And so to me, the people who call it a
privacy paradox tend to be people who are puzzled by
the fact that consumers would say, I like X, and then
when they’re faced with choices where they have to
make tradeoffs, they make a different decision. To me, that’s not puzzling. That’s how consumers are all the time. It’s not a paradox. It’s only a paradox if you don’t understand why somebody would do that, and that’s a failure of the researcher’s empathy and not of the consumer.

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

So for those who haven’t encountered it as much, right, this is the notion that our choice architectures, our choice opportunities are just completely muddled and clouded by the little tricks that companies play to get you to consent, even though you may not want to. And so this is as simple as putting the yes button in a really prominent dark font and the no in a grayed-out font which is harder to perceive. They’re kind of more dramatic examples that
Woody Hartzog talks about in his book. Yes, I would like your health service; no, I just want to bleed to death. And so there’s all sorts of kind of behavioral cognitive tests.

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

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

And I think what we will lead to -- and I think it will be in a way that even the economists will kind of have to agree with -- that there are some
devious tricks that are played at that moment that
to really do undermine the fundamental notion that this
is a contract, this is something meaningful, and this
is something that we should premise, for example, FTC
lack of enforcement on. And so I think mine will only
be one of, like, four or five studies, including some
empirical work on this. And I think people on the
Hill are probably likely to pay attention as well.

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

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

So when we think about either an ex post,
maybe harms-based approach or an ex ante regulatory approach, what do you think is the right way to go, or a hybrid of both, or you don’t have an opinion?

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

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

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

MR. COOPER: Okay.

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

So something based on notice and consent and choice isn’t likely to be meaningful enough, partly because I think the political process will water down anything like that so much. I’m happy with
California, and I would like to see it continue to be the law of at least that land. And so let me just say one thing about ex post and ex ante. For ex post, yes, we should continue to be aggressive in our enforcements. We should kind of do more with the dark patterns that I was just talking about. But ex ante, I actually have always said, and I think I depart with a lot of privacy advocates on this, that there should be more laws tailored to sensitive information, so we should have new laws that kind of find the little gaps in types of information that are so deeply sensitive, so connected to provable harm, and yet for some odd reason we don’t protect in this country.

And so the most obvious one is location information. I mean, there ought to be -- and I don’t care which one, any of the right to location privacy acts that have been proposed over the last few congresses, but there should be a kind of fundamental ex ante restriction on what we can do with the specific accurate location information of people. It doesn’t mean we would, like, drive out of business any company premised on location information, but it means we would really ramp both the notice and choice that’s required, but more importantly the kind of
substantive obligations about what to do with location
information. It should be like HIPAA; it should be
like FERPA. And it’s kind of crazy to me that it’s
not.

MR. COOPER: Well, thanks, Paul.

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

MR. CHILSON: Sure. So I’ll take the
opportunity to be in slight agreement with Paul,
that’s always nice. You know, I do think that ex post
has a lot of virtues in the ability to focus on -- to
address the challenge of not being able to predict the
future, and setting big abstract frameworks into place
based on how the technological world works right now
is very, very, very difficult. And in 10 years, I
think a lot of those frameworks will look out of date
And so ex post approaches that focus on what is a particular type of harm that we’re worried about or what is a particular type of use that we’re worried about, and we’re going to watch and see how companies behave, and then if there’s injury to consumers, we bring actions. I think that approach has that virtue of not having to predict the future as much. It also has the virtue of not having to be as abstract.

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

And on the dark patterns point, if I can just jump to that, I mean, this is not new to the FTC. The FTC in ad practices does this all the time, right? There are all sorts of dark patterns, and in DMP where -- dark patterns where people get involved in loans or they get involved in advertisement for supplements where there’s all these patterns around them. And so
I think that’s great work. I think there’s a lot of evidence that the FTC can draw on around that issue. I think that those parts of the FTC’s work have shown that economists bring a lot to the table there and that when you’re focusing on --

MR. COOPER: Thank you, Neil.

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

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

MR. COOPER: Thanks, Neil.

And, Alastair, I wanted to move to let you react and also just maybe talk specifically about the CCPA. Obviously, that ended up as an opt-out regime. And I’m curious of what sort of considerations went
into — I mean, it’s opt-in for 13 to 16 and then parental opt-in for under 13 because it’s in with COPPA, but for anyone over 16, we’ve got an opt-out regime in the CCPA.

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

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

And so we were and are pretty agnostic about — we believe in the consumer, and we believe the consumer can make that relationship with the first party. And so we don’t put restrictions on the collection of information by that first party. It’s just, you know, the promulgation of that information all the way out into the system where people don’t have any control of it and they don’t understand or
have any control over what’s going to happen to that information. And that’s where we drew the line, and we said we should give people the right to stop the sale of their information.

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

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

We do have a limited private right of action, right, when calling negligent data breaches, which is just like the cop when he stops you speeding, he doesn’t ask you why you’re speeding, he just gives
you a ticket or she just gives you a ticket. And that’s kind of where we are with the data breach. I do think that the whole problem with, like, how were you harmed, Equifax, you know, this data breach, try proving to Equifax that your, you know, identity was stolen six months later because of that data breach.

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

And that’s also why I’m convinced this has suddenly gotten so much attention because companies realize that, wow, this is going to be -- we’re profiting immensely from selling everybody’s data, and we can’t let them have this power to opt out of the sale of that data. And I’m convinced also that these companies are going to do just fine because, again, we
don’t stop the company from collecting or using the data on their own. So if they can make an argument to you that they need to have your data -- Uber does need to know where I am, Uber does need to track me, Uber does need to have my credit card information, great, that’s fine. But do they need to sell it? That’s the second question.

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

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

And then my exhortation to kind of my copanelists is stop challenging and, you know, funding challenges to actions like in the security space. I
know this is the privacy conference, not security, but
if we want an ex post regime that works, we can’t have
kind of these pointless, endless litigation about
whether or not Section 5 even applies to security.
And so that ties the hands of a lot of the enforcers.
Ex post can be a lot more than it has been were it not
for the challenges like that.

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

And I somewhat disagree with Alastair. I
don’t think that all of the companies that are worried
about the CCPA or the advocates who are worried about
it are worried about it because they sell consumers’
data and they think they’re going to lose money. I
think there are lots of reasons to be worried about
the implementation costs of CCPA. And I’m not a CCPA
expert, and you certainly are, but I’ve heard many
more concerns from many people who don’t have a stake
in selling consumers’ data about the compliance costs
that will come about from having to undertake the
efforts that CCPA requires.

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

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

If your business model is based on making a
lot of money from selling your consumers’ data, well,
they don’t think that their consumer -- their data is
being sold, I think that’s going to be -- you’re going
to have a problem. I mean, I think, look, I think
that to go back to this idea of, you know, regulation
and the cost of regulation, I think what happens is
technology always outpaces society’s ability to
understand it.

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

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

I think this is sort of a similar scenario
where right now there has been no regulation, no
really effective regulation around this space in
privacy. And I think California is showing up with some effective regulation. And I think, you know, companies are doing what companies always do when there’s regulation on the horizon. They say, oh, look at the cost; it’s going to be a disaster; people are going to lose their jobs. And the reality is these companies are going to do just fine. They’re going to make money.

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

MR. COOPER: So another audience question, and this kind of goes back to something Paul had talked about earlier, and it’s really more pointed and specific. Do you think that the dark patterns, the
FTC has sufficient authority under Section 5? I know you and Neil had a little back and forth about that. Do you think that there needs to be something additional, or would it fit under current unfair deceptive acts and practices?

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

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

And so they might be, you know, well, you opted into this and look at all the benefits you got, but you really didn’t opt into it because the dark pattern interfered with your ability to make a real choice at that point, right? So, I mean, it’s a
little round trip through FTC doctrine to make it relevant, but, again, it’s couched in the language of economics and so I think has a better chance of kind of having some sort of change within the Commission itself, right?

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

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

MR. CHILSON: Yeah, absolutely. I mean, I think the effect of regulation on competition isn’t
just about changing people’s business models. Often, it is a way that companies use to cement a business model in place when they are afraid of competition. And so I think Alastair is 100 percent right that the big companies will continue to make money here. I think they will then use that money to use a regulatory framework in the way that they are free and open to do through lobbying to protect their interests.

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

And so I do think that there’s that challenge that regulation can often cement business models into place, that the market pressures, which I think we’re seeing there are pressures in this space.
for companies to act in different ways, that market
pressures would push towards naturally, and companies
can use regulation to hold back that change.

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

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

MR. COOPER: We are basically -- not
basically, we are out of time, but I do want to let
Alastair and Paul jump in if they want to have one
last comment.
MR. MACTAGGART: Two things on that. That with all due respect that last comment about having to collect additional information, in multiple places in the act it says that for a single, one-time transaction where you’re not collecting personal information, you don’t have to collect additional information. This is the kind of thing that people throw up to say, you know, this is going to be a disaster, but if you’re collecting personal information, then you’ve got to be able to re-identify it. But if you’re not collecting personal information for a one-time transaction, there’s no requirement to keep it.

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

If Google and Facebook can’t ubiquitously track you across every single thing you do on the web,
that will have a tremendously pro-competition effect.

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

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

And so if the FTC can use its prosecutorial discretion, for example, to go more after giants than after tiny startups. I’m all for that. I think that’s a great policy to enact at the Commission.
MR. COOPER: Okay. All right. Well, join me in thanking our panelists for the time and great discussion this morning.

(Applause.)

MR. COOPER: And we will have a break until 10:45.
THE DATA RISK SPECTRUM: FROM DE-IDENTIFIED DATA TO SENSITIVE INDIVIDUALLY IDENTIFIABLE DATA

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

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

And before we begin the discussion portion of our panel, which will be most of our time together, Jules is going to start us off with a short presentation that covers some of the basics of de-identification, what it involves, what are some of the relevant standards, and what are some of the challenges to de-identifying data.
So, Jules, could you please start us off?

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

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

So let’s look a little bit at just a couple of these, and then we’ll try to pull out some of the learnings from them that help us frame what is personal and what is de-identified. Let me start with one close to my heart because it led to me becoming
the chief privacy officer at AOL many years ago, the researcher who shared online for researchers, a Ph.D. working at the company who shared for researchers a data set where he had eliminated the screen name -- the AOL screen name -- associated with months and months of search results. Probably not any data set that a credible de-identification expert would consider anonymous information, but a young, smart, noble, you know, Ph.D. said, well, there’s probably no risk in putting this data out.

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

More sophisticated and perhaps more interesting for our analysis is Latanya Sweeney’s work, Arvind Narayanan and Vitaly Shmatikov work where they conducted what are known as linkage attacks. What is a linkage attack? Well, when you have a de-
identified data set and it’s joined with a publicly
available data set that has information in it using
attributes that are common to both those data sets.
So what was compelling about the Netflix attack,
right, Netflix released for its prize, testing the
ability of the public to come up with better
algorithms, movie ratings, and dates. Hmm, doesn’t
seem like a very high-risk set of information, and
there wasn’t even a lot of it, which was one of the
critical sort of pieces. It was simply a number of
ratings and dates.

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

They identified two people because they had
a very small sampling. But what they proved was, look
at that, these are easier to do than you might have
thought. This can be done with a fairly small amount
of data and, beware, there are all sorts of data sets
out there that you may not be aware that could
contribute to a linkage attack like this.

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

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

Interesting to note that if one had followed
the HIPAA standards, one would not have released a
data set that would have included that level of precision. It would have had just, perhaps, birth year and the first three of zip, which might have made that attack much harder.

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

Yes, we might have a John Smith, which doesn’t tell us a lot, but is there information that if I look at it without any further research, I can identify this user or can I cross link this information in a trivial way to other information in the public domain? That’s a definition from the IS -- one if the ISO standards. Experts might add “or widely available,” right? So I may not have your name, but if anybody can go ahead and just look up that code online or maybe by paying a small fee, perhaps it’s widely available, obviously on its face,
we’ve got an identifier that is personal.

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

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

I’m leaving aside for the moment now some of the de-identification risks such as we saw recently with the census, where although the census was releasing statistical data, the fact that there were
so many multiple data sets that could be overlapped
enabled experts to narrow some of those cells enough
to make smart judgments about individual users. So
it’s clear that perhaps much of the interesting debate
here is less over what are direct identifiers and what
happens when I make data sets public where clearly
every possible risk needs to be considered, but what
happens -- and this is a chart that we did a number of
years ago that tried to take a look at how does data
actually exist at organizations sometimes.

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

So on the next couple of slides, I simply
want to show how some of the debate, which ends up
being around that outer boundary, do we actually care
about covering this data in law? Do we want to
protect it at all, ends up missing perhaps some of the
more robust debate, which is, yes, we do want to
capture it because it’s probably not a data set that
we’re comfortable making public, but once we do put
rules and restrictions, what comfort level do we have,
whether we call it personal or pseudonymous or
something intermediate because frankly it is in many
cases a spectrum of risk, what are the rules we want
to take?

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

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

I’ll just quickly mention, then, the HIPAA
data, limited data set, where, again, recognizing that
there are valuable research uses if data is controlled
by contracts and not made public, again, although
covered by HIPAA, treated much more flexibly,
similarly under human subject protection, under the
common rule. We’ve got that flexibility under FERPA.
Again, the definition swept wide, but significant
carveouts to support the kinds of activity that
researchers or others might want to do.

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

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

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

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

And then, frankly again, another area where researchers are increasingly excited, using homomorphic encryption, a method of being able to combine fully encrypted data sets but yet do your calculations and have valid information. Again, useful for some valuable uses and not for others.
So just quick final thoughts. Are we talking about public release, in which case, clearly we come to it with the set of concerns that we can’t anticipate every possible method of indirect identifier, we can’t anticipate every possible additional data set, and what is our standard? A flag to one of concerns, we certainly have cities today that are eager for smart city regulation, for other scenarios, to capture data sets, for instance, around location. And those data sets, although the city may feel they’re confident that they’re protected, are subject to Freedom of Information Act requests, might be available for law enforcement, and obviously we’ve seen risks there.

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

So final slide, since so much of the debate, whether we want it or not, ends up being focused on targeted advertising and behavioral advertising. And
we’ll talk a little bit about it, I think, during the panel, but let’s just look at how this framing of is this a direct or an indirect identifier, do we have controls or not that we can trust end up being applied, right?

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

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

And, then, let’s switch to the control side. Are there controls in place -- and maybe for some uses we can talk it -- there may not be -- but other methods of collection with other controls. Maybe
there are ways to bound it probably in the bucket of how do we want to treat pseudonymized data.

MS. HAN: Great. Thank you, Jules. So you had mentioned GDPR’s anonymization requirements.

Aoife, can you tell us about Tr ata and its approach to de-identification and GDPR compliance?

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

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

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

What was the genesis of Tr ata? Well,
anybody who was looking ahead and looking at the GDPR in draft could see that to do analytics under the GDPR was going to prove to be challenging. One of the reasons for that is some of the foundational principles of the GDPR are around purpose limitation, data minimization, and data retention, all of which make it very challenging to collect data for analytic purposes because for analytics you want a large volume of data and you want historical data. And that runs counter to these principles like purpose limitation.

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

Also, when you look at trying to do analytics, many companies have decided rather than trying to rely on consent that they would look to
anonymize the data for the purposes of conducting analytics. But, again, the GDPR raised the bar and made it more difficult for companies to do anonymization, particularly where they were trying to do anonymization in-house.

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

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

We talked about some of the safeguards. When Tr ata was being designed, we really started with a blank sheet of paper. How do we create a company that’s going to operate independently and is going to be able to anonymize the data but to retain utility? How can we design and architect a company that will ensure that we identify the risks of re-identification
and then build in safeguards into the company to ensure that every step along the way we ensure that the risks of re-identification are identified and mitigated and that we can operate independently?

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

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

In addition, then, we have organizational controls in place. Everything from security by
design, privacy by design, and privacy by default have been embedded into the organization in terms of the design and also the operation of the company.

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

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

And once we understand the data, we also understand the direct identifiers and the indirect identifiers. And what we ask the customer to do is to tokenize those and add a salted phrase. The customer then transfers the data securely to Tr ata. And once they’ve done that, they delete the extract of the data set that they’ve sent us. We then doubly de-identify the data by also carrying out tokenization and by also a salted phrase. And at that point, we also delete
And this is an important point to mention in the journey because at this stage, we’ve broken the linkability back to the original data set. The customer still holds the original data set, but now the data that we hold, we’ve broken the link back to the original data set.

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

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

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

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

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

So we are agnostic in terms of the sectors we work with, the various industries we work with, and
the various use cases that a customer might want to use the data for.

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

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

MS. JILLSON: Great. Thank you very much.

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

Michelle, I know you have thought a lot about these issues and that in its proposed legislation, CDT has tackled some of these issues head on. Could you tell us a little bit about that
approach to legislation and why CDT has taken that approach.

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

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

One, we want this to be a really holistic look at data use. If we’re going to do this once, probably right and set the parameters, we want this to be broader than we’ve thought about privacy in the US in the past, what’s really more of a consent model. And so that means looking at data use beyond the
individual and harms beyond whether a single individual can be tied to data that has some harm in their lives.

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

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

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

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

And I think we understand that de-
identification is going to be a big part of the debate
once legislation gets moving this year, and we would
courage Congress to avoid granting get-out-of-jail-
free cards, especially for things like pseudonymous
data. Processing is becoming more sophisticated, and
it’s going to be much easier to re-identify this
information and make really high-stakes decisions about people.

MS. HAN: Great. Thanks, Michelle.

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

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

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

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555
clinical trials and then ultimately to be able to have that data used for research purposes so that what they’re going through is not -- you know, that they can essentially donate their data so that the people coming behind them have a better chance.

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

So whatever techniques that we will use to de-identify data -- which we will because we want to provide our users with options about sharing de-identified data, and we want to be able to when we present that option to them to tell them your data has been de-identified in accordance with some ideal standard that is out there and measurable but also letting them know that de-identification does not
reduce risk to zero, that there still is some risk that that data could be re-identified, and are they still comfortable making their data available for that purpose.

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

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

And we will take some cut from that,
essentially, a broker’s fee of putting patients who
have valuable data together with people who want that
data. And that data doesn’t have to be de-identified
necessarily in order to create that monetization
opportunity. In fact, a lot of times for a cancer
patient, what is valuable is the identifiable data,
but obviously it’s a challenge to make that clear to
folks because these issues can be quite complicated,
but that is our plan for moving forward, is to give
people choices, even with respect to de-identified
data, and then also to be very transparent with them
about what it means for data to be de-identified in
terms of their risk.

I thought Jules did a great job around
talking about HIPAA and particularly emphasizing that
the re-identification techniques that Latanya Sweeney
used of Governor Weld’s data were done before HIPAA’s
standard on the safe harbor was established. But
having said that, you know, HIPAA has in some respects
stood the test of time with respect to, you know,
health data that is generated in the traditional
healthcare system, traditional actors in healthcare in
the United States, doctors, hospitals, health plans,
pharmacies, not pharmaceutical companies because
they’re not covered.
Nevertheless, it’s a standard that was created in 2000. And even at the time that it was created, the agency -- the Department of Health and Human Services -- got a lot of questions about whether they should decline to regulate data that were de-identified. And it’s kind of amazing actually some of the preamble language around the promulgation of that very first privacy rule where they came up with the two methodologies for de-identifying data. And, again, the Department was specifically asked, there is no zero risk. And they absolutely acknowledged it, even at the time.

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

And, then, again, two methodologies. Safe harbor, take out 18 specific identifiers and have no
actual knowledge that the data set can be re-
identified and you are home free. The regulations
disappear. And because HIPAA then doesn’t regulate
that data, it will be subject to potentially
additional regulation by the Federal Trade Commission,
for example, if their jurisdiction applies in that
particular context. But, again, the data has at least
been de-identified in accordance with one standard.

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

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

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

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

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

I’ll make one more point and then I’ll stop, and that is safe harbor has been the method of de-identification that has probably gotten the most
amount of criticism with respect to the HIPAA standard
because it sort of treats -- again, it was created
back in 2000, identifies 18 categories of identifiers,
a few of which are broadly stated, but nevertheless
the assumption that you can create a standard in 2000
and think that it is still as viable in 2019 as it was
at the time just feels a bit -- is naive the word to
use? I’m not sure that that has necessarily stood the
test of time.

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

And that, to them, was a sort of magic
combination for encouraging again less-risk data to be
used for a broad set of purposes, which in healthcare
is often really critical. I mean, that’s one thing
that is somewhat different about healthcare data is
that it has both the potential for serious misuse in
terms of it getting out and people knowing private
things about individuals, but on the other hand there
First Version
Competition and Consumer Protection in the 21st Century

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

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

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

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

MR. WILEY: Well, great. So, one, thank you to the FTC for inviting us here today. Thank you to Paul Ohm for setting me up as the guy representing a
location intelligence company. So Cuebiq provides marketers location-based, artificially intelligence-driven analytics and measurement to map and measure the customer/consumer journey, helping marketers answer strategic questions and make the right decisions in order to help influence consumers through the sales funnel.

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

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

The risk within precise location data is the data itself can in some cases be used to link to publicly available records to reverse engineer...
identity. Not going to go into it deeply, but reference a 2013 MIT, you know, study that looked at this problem and demonstrated that with as few as four location data points, they could reverse engineer identity to about 95 percent of the data pool that they were investigating.

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

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

And then on sensitivity, this is the more difficult discussion point because there’s so many different points to touch on, but location sensitivity poses interesting challenges when compared to content or interest-based category sensitivity. Not to say that those are black and white areas either, but
location sensitivities, you know, have additional dimensions of complexity.

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

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

So at Cuebiq, we call that the Cuebiq ID. But there’s nothing within that ID that would allow me to reverse engineer it back to the mobile ad ID. It’s not a direct hash or a direct salted hash of the
original identifier. It’s purely map table-driven. That way, if I delete that entry in the map table, at least the identifier, there’s no pathway back to that original mobile ad ID.

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

Now let’s get into location information itself. I’m going to put it into three categories, this is sort of how we think about it at Cuebiq, but I think you could use these and express them in other applications as well. The three buckets are going to be in sort of a state-of-art concept or acronym in location data is POI, or points of interests. So if you hear me use that acronym, just add that to your acronym soup for today. But POIs fall into sort of three categories for us. We have known nonsensitive, known sensitive, and then unknown. So a known nonsensitive would be something like Macy’s,
Starbucks, McDonald’s. This is a retail location that we know a device has visited. We don’t deem it to be sensitive.

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

With home and work location, a de-identification technique we use -- and, again, this is borrowed from differential -- privacy is consistent randomization. So in the US, the US Census created a great construct for us to use. If you break the hierarchy down for how information is tracked within the US Census, it starts with a track, then it goes to a census block group, and then you get to the census block itself.
Now, if you’re trying to find a way to sort of group them, a census block is most analogous to a postal code, a full nine-digit postal, five-plus-four-digit code, which generally is city block/side of street. So that’s how specific generally zip-fours are. There are places that break that like New York where you can have very large multistory buildings that have multiple, you know, zip-fours of their own. But generally in the United States, that’s how we break it down.

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

As we move to the last category of unknown, this is where we use consistent randomization in a different way, but this is -- again, we don’t know where this location resolves to, right? It could be in the middle of a field, the middle of a freeway.
It could be a point of interest that we’ve just not yet categorized. So before any of that information would be shared, like through our “data for good” program, where we work with government and academic institutions to help, you know, with programs like city betterment or disaster relief efforts, we do find a point. We take the actual lat/long and randomize it both on vector and on distance within that area. And, again, here, census block group can work.

More interestingly, on the scientific side, we’ll use something called a geohash. If you’ve never heard of that, it’s more of a grid-based way of looking at our globe, where there are different rectangles and the level of the geohash dictates the size. Our general randomization is on geohash level 6, which is about a 1.2 kilometer by .6 kilometer rectangle. But that way we can take these unknown locations, move them into a random point within that geohash 6 rectangle, preserve some degree of path analysis, but again never know that someone dwelled or visited any specific point within that geohash 6, so sort of protecting the unknown sort of category. So that’s sort of a general way of looking at de-

identification. I’m sure we’ll go deeper on that today.
On sensitivity, this is one that we struggle with, I would say, the most. Struggle in that there are no bright lines. I think it’s very clear and easy for reasonable minds to agree on the black and the white side spectrums of sensitivity. Even when I was at Yahoo and we had our sensitive categories council, this was always one that was interesting from a debate perspective and from a cultural perspective on who would find what category sensitive versus not.

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

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

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

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

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

MS. HAN: Thank you.
So I would like to push a little deeper on the topic of sensitivity and direct this next question initially to Michelle, but then I’d like to get the thoughts from the rest of the panelists as well.

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

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

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

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

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

And this is the type of information that we would recommend you put purpose limitations on, right? So if you get to the second part of the question of, well, then, what’s the consequence for being sensitive, we think this is the type of thing that could be clear and actionable for actors, all sorts of
sizes, and gets us outside of the consent loop that we keep being stuck in otherwise when we talk about privacy laws so frequently here in the US.

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

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

And so the reality is, drawing the line
between all the other categories that may or may not
be sensitive or might be sensitive for particular use
and not for another context or with the particular
user ends up, I think, being enormously challenging.
The legitimate interest notion that is actually the
center of GDPR in most uses, even though we talk about
consent an awful lot but is the basis of the sort of
the engine of GDPR, forces that sort of assessment
depending who you are and who the user is and what the
risks are, and you’ve got to document that.

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

So I’d argue there’s a set of special
categories that we all agree and that’s more likely to
be a narrow set that demands, you know, a higher
standard with an appropriate hard-to-get safety valve
for the sorts of uses that are truly defensible and
that the rest of this bucket, because everything can
end up being in there, one location, it could be an
abortion clinic, the ad targeting example that was
mentioned earlier, clearly, you know, highly unhealthy, but can somebody be targeting all facilities where someone might want a ride share ride home, right, or where someone might be selling, you know, some particular, you know, air conditioning device and you’ve got different categories because there are some reasons to logic, though?

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

MS. RICHARDSON: Well, actually, let me push back. I think this is the concern, right? If it’s just a process, I’m afraid it’s going to sound exactly like what we just heard, that it’s different for every individual so actually we can’t create any presumptions on certain data sets at all. If we can’t get to that point during this process, I’m not sure the value of passing a federal privacy law and that
there have to be some baseline protections for certain
types of data. Otherwise, it will not be worth the
trade that we’re asking for here, right, to intervene
and repeal probably 50 different state laws on data
security and privacy.

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

MR. WILEY: Yeah, just to speak to the
sensitivity spectrum a bit, so at the NAI, we spent --
this is circa eight years ago -- we spent a good solid
three years trying to develop a sensitive categories
list. And it ended up being so subjective and, again,
even in the broadest swath’s language, how language
use may describe or not describe something, blood
management versus diabetes, there were so many
difficulties in that process that we went a different
route. And we decided that anything that was suspected to be sensitive required transparency. Let the world judge. Let your users judge.

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

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

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

MS. JILLSON: So in the interest of time, let’s move from sensitivity to de-identification. And could you advance the slide, please? So in 2012, in
the FTC’s Privacy Report, the FTC laid out this framework. The data falls are -- data falls outside the scope of the framework, that is, it’s not reasonably linked to a specific consumer, computer, or device if these three conditions are met.

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

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

MS. MCGRAW: I have some questions around the company requires -- I remember this in 2012, and I’m sure I applauded it at the time. And now that I’m inside a company, I have questions about number three. The company requires any downstream users of the data to keep it in de-identified form. That puts a lot of pressure on companies to chase down all the places where it potentially would be accountable for what a downstream user does with the data, whereas if this
were a sort of more universally applicable standard
that applied to recipients and said if you have it --
if you received it in de-identified form and that is
the basis upon which you process this data, then you
have to keep it in that form and can’t reidentify it
as opposed to always putting the onus on the
discloser.

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

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

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

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

So I think we should be expecting much more
of them. As far as sort of the downstream uses, I
think we need to say not just contractual obligations
for the third parties that you give in a private
space, but if you are going to make the information
public, for example, right, or maybe throw it up in
your API where literally millions of developers are
interacting with it, you are then taking on a burden
and a forward responsibility to make sure that information stays de-identified.

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

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

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

MS. SEXTON: Sure. Thank you. Yeah, so first of all, I think in order to look at the controls, I think you have to look at the risk of re-
identification, and they will obviously then inform what are the level and the robustness of the controls you need. So clearly, if it’s a release of a public data set, then the controls you’re looking at will be a higher degree of controls versus perhaps data that’s just being released intragroup, or as in the case of Tr ata, is it a public release of data but just back to a customer in an aggregated form?

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

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

Obviously, the technical level of controls
are incredibly important. And this is where the real expertise of the data scientists come in in order to really look at what tools are available to them. Jules mentioned homomorphic encryption, and that’s an encryption that’s available to help with the security of the data.

And, also, you’re looking at differential privacy. So there are new tools that are being advanced that will help. So really the level of sophistication of the data scientists will result in the more robustness of the anonymization itself. It is difficult to talk about audits because there isn’t a set threshold, even under the GDPR. There isn’t a sort of a threshold that says if you reach X, therefore, you’ve definitely anonymized the data. So from that point of view, it can be difficult to look at, say, audits to ensure and to specify that you have achieved the levels of thresholds. But I do think that it is a combination of the technical sophistication and expertise together with the combination of safeguards, be it on the contractual level, be it an organization security level, having access controls in place, ensuring that only people on a need-to-know basis can actually access data.
And then in our case, obviously, we’re an independent third party. We are motivated to ensure that we achieve a level of anonymization in a way that’s perhaps different than if you just have the data in-house.

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

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

I’d argue the FTC definition allows controls
to be used to guarantee, if you can, because you’ve got the ability to limit what partners do with it, the use of any of those indirect quasi-identifiers, the data that is interesting, which hospital did this happen into and so on and so forth, and allow you to treat that, whether you call it pseudonymous or protected pseudonymous or whatever you want to call it.

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

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

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

Another audience member asks about data uses
and if that should be taken more into account when data is nominally de-identified but it results in an adverse impact on someone.

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

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

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

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

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

What I was trying to chime in on is contractual controls, and, frankly, we use them and we’re subject to them, but they feel like CYA, weak tea to me because once you get, you know, thousands and thousands of contracts, how can you possibly go out and chase those down? I would much prefer an environment where whomever we give our users’ data to, with their consent but nevertheless knowing that
consent is not enough, that they are also bound by a 
set of obligations to act ethically with respect to 
that data, as opposed to me contractually making them 
do it and then having to chase that down when they 
don’t.

MS. JILLSON: Well, thank you all. I’m 
afraid we are out of time, but my thanks to all of the 
panelists for a really interesting discussion. 
And we will now take a lunch break. We’ll 
be back at 1:00 for another set of panels this 
afternoon.

(Applause.)
REMARKS - NOAH JOSHUA PHILLIPS, COMMISSIONER

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

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

With that brief introduction, it is my privilege to turn the podium over to Commissioner
Phillips.

(Applause.)

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

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

For those who’ve been studying and advocating on these issues for years, many of whom are
with us today, I hope this is a welcome development. I think it surely does reflect a great deal of perseverance on your part. But for many policymakers, for lawmakers, and for consumers, our consumer data privacy moment seems in large part to have come out of nowhere, and in a short time at that.

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

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

So that’s why I said at the beginning, the hearings that we are holding this week are critical to the national interest. And I’m particularly pleased
to see that they began today with a topic of the first panel, a notionally modest but actually difficult and essential step, defining the goals of consumer data privacy.

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

Rulemaking penalties, funding, these are merely tools. It is the substance, the harms we are addressing, and the rights that Congress intends to create to address those harms that require our primary attention. Privacy is a nebulous concept, and different people can and do conceive quite differently how individuals are harmed by a privacy violation. They also differ whether and to what extent they experience a given kind of conduct as a violation and then how much they would pay to avoid it.
Are consumer data privacy harms limited to physical injury and financial loss? Do they include emotional distress? Is a sense of surveillance or creepiness characteristic only of an eggshell plaintiff, or is that something Congress needs to prevent? What about a lack of empowerment or a loss of control over data? And how, if at all, do these things take us back to Brandeis’ and Warren’s famous right to be let alone.

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

When the NTIA surveyed Americans in 2017, the number one harm they reportedly feared, or we reportedly feared, was identity theft. That makes sense to me. And that is why I think the most significant thing we can do for consumer data privacy is to improve data security. While we often discuss privacy and security disjunctively, they are, in fact, close relatives. And all five FTC
Commissioners agree on the need for data security legislation, including having the FTC’s authority in this area codified, providing us with civil penalty authority to enhance deterrence and giving the Commission jurisdiction over common carriers and nonprofits. Moving that legislation forward would be a major win for consumers and a major accomplishment for privacy.

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

I focused in my remarks today and elsewhere a lot on Congress, and that is not by accident. Some months ago, I was invited to address the Privacy Coalition at EPIC’s offices and answer questions. After I gave a similar spiel about the need first to agree upon privacy harms that we would address, a participant asked me why I was focusing on harms and
not rights. That is a great question. And the answer cannot be more important.

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

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

But this is precisely the point. Congress needs to make those rights. The framers of our Constitution, who established a republican form of government that has lasted for centuries and that remains today a symbol of liberty and economic success
the world over, relied heavily for inspiration on the philosopher John Locke. In 1690, Locke famously wrote -- this is a quote -- “The power of the legislative, being derived from the people by a positive voluntary grant and institution, can be no other than what the positive grant conveyed, which being only to make laws, and not to make legislators, the legislative can have no power to transfer their authority of making laws and place it in other hands.”

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

I am concerned about the impact on the market of a set of far-reaching rules that could morph with electoral politics. Businesses, whether they like a particular law or not, need certainty and predictability so they can plan and make investments. These are crucial for them and for our economy. If substantial changes to the law are in the hands of
just five people, the chance the rules of the road will change back and forth will, on its own, chill economic growth. And I’ll add to it. I don’t think it’s particularly good for the agency to have to deal with that on a regular basis.

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

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

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

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

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

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

I want to end on what for me is a critical point. We, as a society, are undergoing a major shift in how commerce is conducted. And however
uncomfortable that may make some of us, it’s not going
to go away. We’re not going to succeed like the
samurai of old in keeping the guns off the island.
And by the way, that didn’t ultimately work for them.
And no matter what laws Congress passes, in a sense,
they will never be enough.

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

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

So here’s my pitch. The discussion about
consumer data privacy is one of the most complex 
 policy debates we have had for a while. Likely with 
 dramatic economic, political, and social consequences. 
 There may be no do-overs if we get it wrong. So 
 let’s go forward deliberately and carefully, taking 
 short-term wins where the consensus is clear, as in 
 data security, and making sure we are evaluating any 
 new privacy regime with data and careful analysis. 
 And let’s work on developing a shared framework that 
 helps consumers and businesses understand the value 
 of consumer privacy so that any consumer data 
 privacy legislation is built on that framework of 
 shared values and a recognition of the importance 
 of privacy.

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

These hearings are a great example of the 
 discussions that I think we need to have -- maybe the 
 best example. So to those of you in this room and to 
 those at home who are watching, to people who have 
 submitted comments or otherwise engaged, I want to say 
 thank. Thank you for engaging and debating, for
putting meat on the bones of this privacy debate. And
I look forward to learning from you now and in the
future. Thanks very much.

(Applause.)
CONSUMER DEMAND AND EXPECTATIONS FOR PRIVACY

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

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

MR. GOLDFARB: Rotman.

MS. VANDRUFF: Rotman, excuse me, Chair in AI and Healthcare at the University of Toronto. Beside Professor Goldfarb is Ariel Fox Johnson, who is Senior Counsel of Policy and Privacy at Common Sense. Beside Ariel is Jason Kint, CEO of Digital Content Next. Next to Jason is Laura Pirri, Senior Counsel -- excuse me, Senior Legal Director and Data Protection Officer at Fitbit. And last but not least is Heather west, who is Senior Policy Manager at Mozilla.
During our panel today, a number of my colleagues -- at least one of my colleagues -- will be in the room distributing comment cards. If you have a question or if anyone in our web audience has a question you can tweet it at us and we would be pleased to try to integrate that. Those questions will be moderated through Dan and me.

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

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

MS. PIRRI: Sure. Hello and good afternoon, everyone. So are consumer expectations and demands relevant to privacy policy? I will say yes, absolutely. And I think that in discussing what
customers and consumers want regarding privacy, it’s important to say that companies are very motivated to understand their customers’ expectations regarding privacy so that they can deliver on them. And this is not just because privacy generates customer trust and goodwill but because it is good for business.

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

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

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

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

And not long after that, we launched a data export tool that allowed people to download their data directly from the Fitbit website. So I mention all this to stress that this was in 2011. We launched our data export feature globally. This is well before we
considered the GDPR or any data protection right to
data portability. We did this to satisfy a consumer
need and a demand that we saw within our user
community. We did this for business purposes rather
than for any regulatory requirement.

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

We also learned that for some of our
customers, the fact that we had this data export
feature was a competitive differentiator for us. We
had some customers who purchased a Fitbit precisely
because we had this data export tool. And this was
important validation for us of our early decision to
take consumer expectations regarding privacy into
consideration when developing our products and
deciding how we process our users’ personal
information. So to answer your question, yes.
MR. GILMAN: Thanks, Laura.

Anybody else on this or a different version of this?

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

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

I think that, you know, when we are designing Firefox and when we’re designing the other Mozilla products that we are thinking about, we are doing user research and we’re thinking about what those expectations look like. And I think from a policy perspective, we need to be doing the same thing because most of these problems can’t be solved either technically or with policy. It has to be a marriage of the two.
And our top privacy principle when we’re designing products is don’t surprise the users. And I think that when we can translate that into policy and start building product and policy broadly, for Americans who don’t want to be surprised but do want to use these amazing, cool tools, we start to look at the right answer.

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

MR. GILMAN: Lorrie, you wanted to --

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

And so I don’t know that we can -- you know, when a company says, oh, well, you know, my customers are happy to give me their data or they want advertising, they want targeted advertising, I think you have to look with some skepticism about how are
they measuring this, how are they framing the research
question and who collected that data.

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

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

Unfortunately, some of this is -- some of
this is because of COPPA, which is great, and then
some of this is people don’t understand COPPA and they
think it prevents the collection of any information
from children under 13 or even under 18. But kids,
they don’t really have an expectation of privacy, and
they don’t really have an understanding of privacy. They don’t know that a toy that they talk to is recording them or sending their voice or information somewhere. They may view -- in studies they have viewed GPS and location tracking on devices as sort of a positive thing. And unlike adults, who I think in this past year really woke up and started to better understand what happened with data and how things worked behind the scenes that privacy is more than just, you know, targeted ads, children are not going to have that kind of a wake-up call. And so we need to, I think, work to make sure that they are protected, whether that is their expectation or desire or not.

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

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

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

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

MR. KINT: Sure. Thank you for having me.
And to reiterate, I think there are some really important data points from Ariel. There’s a myth out there that younger people don’t care about privacy, and it’s quite the myth, so I’m glad you popped that with some stats.

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

Michelle Richardson earlier today from CDT very much focused on this goal of maximizing the trust in that relationship with the user. That’s what we’re trying to do, and most of the problems out there, particularly consumer expectations, have to do with secondary uses of data. And that’s what we see as publishers, too. There are certainly companies that publishers work with to deliver on the exact product that the user wants, the service that they’re trying to experience, but when the data is used for other purposes -- that’s why purpose limitations are so
important -- when they’re used for other purposes outside of the user’s expectations, it erodes trust. We are here today, we’re doing these series of hearings because there is an erosion of trust in digital right now, and it comes from very significant things that happened outside of consumer expectations. We have tried to measure those expectations through surveys and research. It’s important to note that the two companies that collect and use data more than any companies in the advertising business, Google and Facebook, they collect data on a majority of the pages on the web. Facebook collects data across over 8 million publishers sites. They’ve disclosed that. Google on over 70 percent of the top 1 million sites.

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

MR. GILMAN: Thanks. I wonder if some of the other panelists can sort of follow up on this
issue that Jason mentioned, and that is how we assess or measure consumer expectations and consumer demands. Obviously, consumers make certain choices in response to offerings. We do various kinds of surveys which may raise other issues, but there’s both sort of what are the background expectations, what do policies mean, what are their preferences. What are some of the different ways we assess the expectations and demand more or less reliable or persuasive in different contexts? Can we get into this sort of assessment a little more?

MS. PIRRI: I can speak to how companies both assess and address consumer expectations regarding privacy in both the context of children as well as sort of more generally with adults. So first in the context of children, Ariel mentions the standards that are set out by COPPA. In addition, companies often look to good privacy-by-design principles. And I can give another Fitbit example, which is that we have an Ace device that is for kids. Our market research showed that parents and kids were looking for ways to encourage healthy habits and to get kids to be more physically active, including through reminders to move as well as step competitions with friends and family. Our research
also found that parents were very concerned about how
their kids’ personal data was being collected and
used.

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

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

The other subject I wanted to discuss, too,
was more broadly with adults and how do we assess
privacy expectations in general. And I think on this
point it is important to stress that privacy does not
necessarily mean private. Sometimes when we discuss
privacy, this is the underlying assumption. And at
Fitbit, we think about privacy as giving people
control over their information, control that we enable
through product features that allows people to make
different preferences regarding how their information
is used.

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

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

So while some --

MR. GILMAN: I’m sorry, Laura. This is
important, I think, and we want to hear more about it.
MS. PIRRI: Okay, let me just get to the bottom line.

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

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

MR. GILMAN: Thanks, thanks.

MR. GILMAN: Avi.

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

The first one is you can ask people what their preferences are. And if you ask people what
their preferences are, they tend to like things that sound good, like privacy and like openness. And on the same topic, you could ask the same question, hey, do you think privacy here is good; they’ll say yes. Do you think openness here is good; they’ll say yes, even though in some sense those can be the opposites.

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

MS. JOHNSON: So briefly, I guess, I think it’s a really important caveat if people are informed and then also if they choose to use the service because I think in a lot of contexts, particularly let’s talk about children again and teens and they’re in school, you have to use certain services to get an education or you have to use certain services for your work.
I know people are trying to see, you know, how long they can avoid Google. You know, I couldn’t have my job and not use Gmail. So in a lot of these instances, I don’t know that we can really see both information and a choice by consumers.

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

And so I don’t -- you know, they’re going to self-reveal before they self-reflect, and so they’re sort of making a choice in that instance. I thought Professor Ohm did a good job talking about if it was a real choice and this question of dark patterns, but I
don’t know that I put a lot of stock in what they might be doing online and whether they really have choices.

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

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

So I actually did research at this point about 10 years ago with Alessandro Acquisti and some
of our students, where we said, well, what if we could really show people in a very easy way what their privacy choices are when they’re shopping online. And so we built a search engine that had a privacy meter in the search results, and so you could see it at a glance. And we gave people money and we asked them to go shopping online and they got to keep the change. And we set it up so that they could shop at the more expensive website to have better privacy or shop at the cheaper website, get the exact same item but with worse privacy.

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

MR. GILMAN: So what’s the response there, right? We prefer revealed preference, all things equal, as Avi pointed out. Information is limited, imperfect. Choices are limited, and not to imply that we ought to be sanguine about these limitations, but, you know, in some ways decision under uncertainty is
ubiquitous. The market may provide a few choices.
There are many choices, but not infinitely many
choices.

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

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

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

MR. GOLDFARB: So first I want to say that
Lorrie and Alessandro’s study is, you know, in some
sense, exactly where we like to be in the sense that
it was revealed preference and it showed a preference of privacy under one situation and not the other. At least my reading of the paper, it’s not obvious which was the right one, but that difference is interesting. But I do think, circling back, it’s important to remember that privacy is one attribute among many, and one thing that we need to think about very carefully is how much we want to elevate that attribute above the others versus not. And related to that, it’s important to remember that privacy is a beneficial attribute, but it’s like other attributes when you’re designing a product, you have these tradeoffs in the sense that search engines tend to be more useful when they can take advantage of data. And social media platform tends to be more useful if data gets shared within the platform. So, you know, there’s certainly places where the costs of privacy are relatively high compared to what the consumer benefit would be, and I think that’s what everyone else has been talking about, but I think it’s really important to recognize there are tradeoffs here, the data is useful, and so in -- you know, in product design, with or without regulation, those tradeoffs should be at the forefront.

MR. GILMAN: Okay. Thanks. Should we move
along? I think this is very good, and I hope
panelists will follow up with us after. I know you
all have a lot of work on this. I don’t mean to short
change anybody.

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

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

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

I do feel that there are also times when a
consumer has expectations that they have no control
and that expectation is met and that can also be a bad
thing, so it’s not just when consumer expectations aren’t met that there’s harm. But if they wouldn’t have done what they did, had they known what you would do with their information or their data, that seems like a harm to me.

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

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

And so on the purchasing point, I will say that one way that Fitbit has been responsive to consumer demand is in how we market our devices. We understand that the data that our devices collect and the functionality that they provide are relevant considerations at the time of purchase. So our website provides information about the different devices that they -- the devices that we, the different data types that they collect, and the
different functionality that they provide. So this ranges from, you know, basic step count, sleep tracking, to more sophisticated features like heart rate and GPS tracking. And consumers may choose to purchase a device that has more limited data collection; however, this means that there may be a tradeoff in that there is also more limited functionality. So our devices that do not collect heart rate data or GPS data don’t have certain -- don’t enable certain features like the heart rate information and the dashboard or the exercise and run maps that are based on GPS data.

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

MR. GILMAN: Thanks.

Jason, I know you’d been trying to get in
the last question. I don’t know if you have --

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

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

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

Most of our 80 or so premium publisher members do things with data as part of the experience that most consumers fully expect. And if they violate
that, they’ll go somewhere else, they have that choice. The New York Times or The Wall Street Journal certainly I think most people want them to recognize you when you come in as a subscriber so that you can actually immediately consume the news and not have to log in every time. But if they violate that data relationship, then you will go somewhere else because there’s real competition in the news category, for sure, and there’s certainly competition in the entertainment category.

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

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

MR. GOLDFARB: So I’m listening here, I’m trying to figure out where the -- think through where the market failure is in the sense that, you know, yes, consumer negative surprises, that’s bad for sure. That’s bad for firms, that’s bad for consumers. But we have some sense that firms do respond. We just, you know, heard how Fitbit thinks about these, and
lots of other companies, I’m sure if they were up
here, would say the same thing.

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

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

MR. KINT : Totally agree. I just want to
lock in on one point there. It is the intersection of
data policy and competition that we think is critical.
And I think Facebook has a company to outline this,
and there’s a great research paper that was put out on
this, is a great case study on a company that led with
privacy for its first five or six years as a company. You couldn’t even use the product unless you were doing an experience that was very privacy protected. The executives all talked about privacy as the most important thing to the product.

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

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

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

Who would have thought their thermostat had a microphone? Once you’ve bought it and put it on your wall, it’s actually not that easy to go buy
another one, take it down, and replace it. So I think that there are many cases where consumers don’t have real privacy choice.

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

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

MS. VANDRUFF: Okay.

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

And so we did a bunch of research, and if you wanted to search for that, it’s called Improving
Privacy without Breaking the Web, and it goes through our entire research process. What do people actually want? What are some of the balancing factors that they are interested in? Does this actually break things?

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

And in the last year, we also created something called Facebook Container, which I think is actually a really interesting use case. And what it does is it divorces your interactions on Facebook as a first party with your interactions on pages that have Facebook as a third party because what we heard from our users is they were surprised that Firefox, their...
browser, who is trying to protect them online, was
facilitating those data flows. And that’s more of a
little bit of an experiment to see how that works and
how -- you know, whether people like it. People seem
to like it. But those are the kinds of tools that we
have been building and thinking about. And so we’re
actually looking for people to give us some ideas
because we want to build those tools.

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

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

There’s other things like fraud prevention,
billing that would fit in that category.

Personalization, if you go into a sports site, it
knows who your favorite sports teams are if you tell

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555
it, things like that. Again, it’s about the secondary uses. The word “tracking” was used by Heather, which, you know, I think Mozilla and Apple are both doing brilliant work and thoughtful work to try to delineate between these two experiences so that they don’t break things but at the same time give the consumer more of what they expect. So I would like to see more positive work there.

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

That’s only because of the way the market is currently designed. If we raise the bar across the entire industry equally, then we will solve for that issue so we can have an experience like what Mozilla and Apple are envisioning that’s even better for the
user, and that’s the tricky part and why the work being done here is really important.

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

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

MR. GOLDFARB: So at a high level, it should come as no surprise that data’s useful. The reason companies are trying to collect data is not because they are trying to violate privacy, per se, typically. It’s instead that the data that they have is useful -- that they could collect about consumers and others is useful to the company. And so restriction, regulatory restrictions in particular, on information flows are
going to restrict the ability of firms to do that.
That said, to the extent that consumers are
demanding it, that actually -- you know, that goes in
the other direction because if consumers trust firms
more then they are going to be willing to give those
companies potentially more useful data or just
generally be their customers, which is what the firm
is trying to achieve in the first place.

MR. GILMAN: Anyone else?

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

And so I think that’s actually where the
California law, and I know you had Alastair Mactaggart
earlier today, where it was really smart is it hasn’t
gotten in the way of using the actual websites as you would want to use them, and it hasn’t gotten in the way of behavioral advertising inside the context of the website. It’s preventing the ability to do secondary uses of data when the user doesn’t want that, and that’s smart.

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

Breakthroughs in health research often come from amassing large data sets of very personal and sensitive information from multiple data sources. So, you know, obviously, there are significant privacy considerations here. At the same time there are social good considerations, you know, that countervail. And the privacy protections that get put
in place or that tend to get put in place to protect
individuals, for example, getting individual consent
as well as aggregating or de-identifying data sets, do
mean that there are restrictions on those research
data sets and inevitably some useful data is removed
from those data sets, some useful data that could have
been used for a social good.

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

MS. JOHNSON: And I think I might just say
that while I agree there are definitely sort of social
good uses of data and it’s not all about the
individual, I think if we’re remiss in not mentioning
that I think the flip side is also true that there are
negative externalities in terms of data being
collected. What might not be a big deal for one person suddenly could be very problematic if we’re talking about a community or a country, and so it sort of works both ways.

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

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

MS. WEST: I think it’s a very interesting way to frame it, but, you know, Mozilla supports the passage of legislation. We published a blueprint for what we think that should look like and it does have a lot to do with consumer expectations, and purpose
specification that Jason’s been talking about is also
a big piece of that to talk about -- okay, so I gave
you my phone number but here’s how I expected you to
use it. And I do think that that’s a good start to
the discussion around how to translate these consumer
expectations and desires and preferences into
legislation or regulation.

MS. VANDRUFF: Anyone else?

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

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

MR. KINT: It’s a good point.

MR. GOLDFARB: So I also think it’s an
intriguing idea. There are sort of two challenges I
can think of. One is not all consumers have the same
expectations. So I think these expectations are going
to be a first-order challenge. And, two, as with
anything, you’ve got to make sure that the regulatory
burden isn’t high enough so that only the big
companies compete and comply at scale. And so however
you design thinking about what expectations are, the
expectations of, you know, you have to make sure that
startups and large established companies can still
compete.

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

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

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

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

MR. GILMAN: Laura?

MS. PIRRI: I mean, you know, I think to
follow up on that, the US approach has very much
historically always looked at balancing considerations
around protecting consumers as well as enabling the benefits of innovation. And so, you know, I think that in order to continue that sensible tradition that looking at ways that technology can put the user in the driver’s seat is incredibly important as we sort of evolve our privacy policy and approaches.

MR. GILMAN: Thanks.

Jason?

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

And so there is enormous power that is moving towards and has moved over the last 10 years to a very few number of companies for much of the advertising sector. And that is squeezing the oxygen out of the companies that are actually creating the news and entertainment that have historically been responsible for the trust of the public. And it’s having societal implications now. That’s why we’re here and talking about it. And so we need to raise the bar quickly and smartly across the industry.
MR. GILMAN: Thanks, Jason.

Ariel.

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

MR. GILMAN: Great.

Avi?

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

MR. GILMAN: Great.

And Lorrie.

MS. CRANOR: I think we have to make it really easy for consumers to be able to understand
what’s going on and exercise their choices. And, you know, the set-and-forget approach is a nice, easy approach, and I know it gets a lot of resistance, but I think we need to find ways of meeting consumer expectations by making it easy for them and to collect data to actually validate that these things work.

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

(Appplause.)
CURRENT APPROACHES TO PRIVACY, PART 1

MS. VANDRUFF: Well, good afternoon, and thank you for joining us. We are continuing our session this afternoon with our panel on the current approaches to privacy. I’m Laura Vandruff. I’m an attorney in the Division of Privacy and Identity Protection, and I’m joined by my colleague, Jared Ho. And let me introduce very briefly our panelists. Their full and impressive biographies are in your materials, as well as online. But very quickly, to my left is Margot Kaminski, and I’m excited that she has a short presentation for us after I quickly introduce the balance of our panel.

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

Again, to Margot’s left is Fred Cate, who is the Vice President for Research and a distinguished Professor of Law at Indiana University. To Fred’s left is Markus Heyder, who is the Vice President and Senior Policy Counselor at Hunton -- excuse me, always Hunton & Williams to me, but it’s Hunton Andrews Kurth at Center for Information Policy Leadership.
To Markus’ left is David LeDuc, and he is the Vice President of Public Policy for the Network Advertising Initiative. To David’s left is Laura Moy. She’s the Executive Director of Georgetown Law’s Center on Privacy and Technology. And finally to Laura’s left is Shaundra Watson, Senior Director of Policy at BSA, the Software Alliance, where she provides counsel and develop’s global policy.

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

MS. KAMINSKI: Okay, thank you.

MS. VANDRUFF: Thank you, Margot.

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

So I’m going to start with an overview of the US federal laws. I’m going to then go to the General Data Protection Regulation, the EU’s data
protection law, and then I’ll talk very briefly about proposed and recently enacted state laws, and all of this in five to ten minutes. Thank you for the laughter.

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

A data protection model, by contrast, follows the data. So there are a series of individual rights, which I’ll get into in greater depth shortly, and company obligations, which track the personal data itself rather than focusing directly only on the relationship between the consumer and the business.
And many models out there, even within the United States, are hybrid models somewhere between the point of the spectrum.

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

We have the contrast between a notice and choice model, which often is employed at some way in the consumer protection model and sometimes within a data protection model as well versus sort of augmentations to notice and choice that focus more on, for example, company obligations or duties, even in the absence of individual invocation of rights. And that goes to a contrast between an individual rights regime that gives individuals notice rights, access rights, control over data versus a compliance regime that focuses more on appointing data protection officers or having data protection impact assessments and not just the duties that companies owe to
individuals but the management and risk assessment regimes for data running through their companies.

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

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

Then we have our federal sectoral statutes, again which I’m sure we’ll talk about at greater length during this panel -- HIPAA, COPPA, the Gramm-Leach-Bliley Act, all of which target either specific entities or specific types of information or
combinations of both. These have data protection-like features. So sometimes there are rules that follow the data as opposed to rules that just focus on the direct relationship between a consumer and a company. But they’re not data protection-like in the comprehensive way that, say, the GDPR is.

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

The GDPR -- wow, that’s small font -- the GDPR, on a very high level, differs in a number of ways from US regimes, as you all know. First, it is absolute an omnibus type of regulation. I’m going to largely talk about it as it applies to companies because that’s the impact for individuals in the United States or companies in the United States, but it’s omnibus in the sense that it follows all personal data and all processing of personal data with exceptions for personal household use for the context of criminal law and the context of national security,
The definition of personal data is extremely broad, rivaled probably only by the definition of personal data in the California Consumer Protection Act. The GDPR represents the data protection model par excellence, right? The laws follow the data. They very clearly apply to third parties that hold data they did not obtain originally from an individual with whom they had a consumer relationship. And that includes especially coverage of third parties. In fact, arguably, the GDPR puts more onerous requirements on third-party data brokers than it does even on the companies that have direct business relationships with consumers.

It’s hard law along some lines. There are, again, famously significant fines that attach if regulators decide to use them in enforcement, and there are both individual rights of enforcement, regulatory enforcement, and serious court involvement. And this is combined -- this system of hard law is combined in the GDPR with softer law which ranges from just the inclusion of broad standards that will eventually get fleshed out through back-and-forth between companies and regulators. And in addition to those broad standards, specific formal mechanisms of
collaborative governance contemplated, like, codes of conduct or certification mechanisms.

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

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

And then the obligations for companies, which form what I would argue is the bulk of the GDPR’s impact, stem from this idea, this core principle from the GDPR of accountability. So this is the idea that companies not only need to institute complex, internal compliance regimes, but they need to be accountable throughout internally and, if regulators choose to ask for it, and for some
mandatory reporting requirements directly to the
regulators.

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

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

In practice, as many of you know, again,
companies often avoid consent because consent can be
withdrawn under the GDPR and instead choose other
legitimate grounds for processing. Obligations also
include all of the above, transparency requirements;
affirmative notice requirements, not just when individuals ask for access, but affirmatively to individuals who haven’t yet asked; documentation recording requirements; security obligations; the requirement in some circumstances, high-risk circumstances, that you appoint a data protection officer; conduct impact assessments; and the famous/infamous requirement of data protection by design and by default, which again is largely a designing corporate governance -- internal corporate governance mechanism type of requirement.

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

All right. So in my remaining few seconds, by comparison, the California Consumer Privacy Act, which you’ve heard about a lot throughout the day, it is somewhere between consumer protection and data protection. So there are elements of it that focus
primarily on the relationship between a consumer and
the business that gathers consumer data directly from
the consumer. And there are other elements of it that
do actually follow the data, which is different from
most US existing privacy regimes.

It’s omnibus but it’s only omnibus-ish in
that it focuses on businesses with the definition of
“business” being a subset of three different kinds of
businesses. The definition of personal information,
however, is broad, extremely broad, and possibly
arguably broader than the definitions within the GDPR.

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

It has a limited opt-out right, again, of
sale of data, but not in other contexts. And its
enforcement mechanisms are very different from the
GDPR. There’s no individual right of action. It’s
enforceable largely by the state attorney general,
except in a specific data security context, and that
state attorney general is also the regulator responsible for promulgating rules that clarify some of the obligations under the law.

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

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

Okay. So, I’ll close here. The proposed state laws that we’ve seen around the country, and
we’ve seen probably almost all of the states impose
something that they call or propose something that
they call data privacy laws in the last year. They
largely, to the extent that they are data privacy and
not just data security under the guise or name of data
privacy, as my home state of Colorado has, to the
extent that they are data privacy laws, they’re
largely directly mimicking the CCPA and not mimicking
the GDPR.

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

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

So, with that, I will turn it over to my
fellow panelists. Thank you very much for your time.
MS. VANDRUFF: Okay. So, that was tremendous. I learned everything I needed to know. No, in all seriousness, that was a very quick overview, but really very substantive. But I wanted to just open it to the panel at the outset to see if anyone had any high-level comments on the differences and approach that you see between the GDPR, CCPA, and the US sectoral-specific approach in self-regulation. And if not, then I can move on to a different question.

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

I think I would highlight a couple differences. So, one is the enforcement of GDPR. So something that GDPR does that is kind of new and probably -- likely will make a big difference in seeing the impact that this law has is that it allows for fines of up to 4 percent of a company’s annual revenue for violations of GDPR. And those are...
potentially tremendous fines, right? I mean, if you look at some of the biggest fines that we’ve seen in the US under Section 5, you’re looking at fines that could amount to hours rather than days or weeks of a very large company’s revenue for violations of consent decrees that have been agreed upon under Section 5.

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

MS. VANDRUFF: Markus.

MR. HEYDER: Yes, thank you. So the one thing that I want to highlight that’s a big difference between the GDPR and the CCPA, for example, is that the CCP -- the GDPR provides for a comprehensive approach to privacy, and the key element to that, I think, is the fact that it codified the concept of organizational accountability, which essentially focuses and forces organizations to develop comprehensive privacy infrastructures that cover the entire data cycle throughout the data lifecycle,
throughout collection up until use and disposition of the data.

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

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

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

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

MS. WATSON: And I just wanted to pick up on I think something that both Markus and Margot mentioned with respect to the accountability piece.
We hear a lot about in discussion of what a new federal law should look like. You know, are you going to replace California? And our response to that question is that, first of all, a federal law doesn’t mean it needs to be a weak law, and we want to actually strengthen the protections that are in CCPA. And when we say that, I think we are sort of referring precisely to what Markus is alluding to with respect to accountability and with respect to what Margot said about sort of regulating the first party use of information.

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

I think another important difference between the GDPR approach and the approaches that we’ve seen in the United States is that GDPR is obviously built on an EU model, a civil code model. And so that necessarily means that the provisions are more proscriptive and more detailed. And what we’ve seen in the US is an approach that strikes a little bit of a different balance and, therefore, you have a little
bit more flexibility in how you do things.

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

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

And so, we see different approaches. Like, we share the overall arching aim of GDPR is to provide consumers with more control over their personal information and to ensure that companies are
accountable, and we share the same goals. But I think the real question is how do we implement those protections in a meaningful and effective way, in a way that is -- fits the US legal culture and legal context. And so I think we’ve seen a number of different approaches, but I think those are some differences that I would highlight.

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

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

And I certainly don’t think that’s the
intent of GDPR, I mean, as written, but it’s the reality. If you look at CCPA, we’ve also got a new law that’s very focused on notice and control. And, you know, speaking on behalf of NAI and the digital advertising industry, those elements, the FIPPs, they’re critical to data responsibility, but at the same time, we really feel like -- you know, Margot used the term “paradigm shift.” I mean, we really feel like it’s time. We need a paradigm shift back towards accountability as Markus mentioned. We need to have privacy laws that focus more on data uses and harms rather than trying to saddle consumers with the responsibility of having to manage their data.

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

And another element I would point out about the CCPA, which I haven’t heard come up much today, is that CCPA is very unusual in focusing on just the sale. So it creates this concept, and I think this false sense of security or privacy to consumers, the notion of, well, if your data’s not being sold, then it’s just fine. You know, if your data’s collected by
a first party, that’s great, you can trust them, but it’s the third parties.

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

And I think, you know, as many of us are looking at the CCPA, how it will be implemented, I think people are going to be very disappointed with respect to, you know, that as a framework and in terms of -- and so when we talk about -- like Shaundra said, when we talk about a federal law, I mean, I think we can look at the GDPR, we can look at the CCPA, try to take the best elements of those, try to take the flexibility from the GDPR that I think was intended frankly that could be implemented, try to take some of the protection -- the protections, the controls for consumers conceptually from the CCPA, make sure that consumers have those, but really focus on data use, on
reasonable uses, focus on those, try to get those out of the system.

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

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

And I think that’s something that we’re starting to see in some of the conversations around where privacy might go in the US, is we’re starting to
talk more about harms that are not necessarily linkable and tangible with respect to the individual. And, David, I actually think that your comments are getting there a little bit, thinking about some first-party uses of data, that some of the -- some of the things that we might find most concerning about uncontrolled uses of information, about consumer information right now might be harms like discriminatory advertising, right? They might be harms that fall more broadly on society where it’s very difficult to see exactly what the impact is on an individual.

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

So, you know, for example, we saw, I think, 44 civil rights and privacy organizations, our organization was one of them, send a letter to Congress a couple months ago highlighting the civil
rights principles in the era of big data and talking about the importance of protecting civil rights in the area of big data and centering these considerations about societal harms in conversations about privacy. But those really are societal harms that traditionally we haven’t seen centered in privacy conversations and maybe haven’t seen centered in these laws.

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

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

And that really is sort of -- those sort of are interests viewed through a societal lens and less through a private -- through an individual lens. So,
again, I think that largely we’ve seen these laws focus on the individual, but we’re starting to see the conversation shift more toward privacy interests that affect society.

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

This is, of course, meaningless today when almost all use of information occurs outside of individual control. Nor would we want to try to control it. I mean, think about a world of internet of things and artificial intelligence and big data, and it’s a little bit silly to think that an individual is going to exercise control or really wants to.
What we want is for our information to be in control, to be subject to some sort of type of protection that will assure us that, if we are harmed by it -- and so, in fact, moving the discussion out of Europe, out of CCPA to instead say, let’s talk about what are the actual objectives, what are the harms we are trying to avoid. Those harms may be physical. They may be financial. They may be emotional. I mean, we recognize emotional harm in other areas of tort law. There’s no reason we wouldn’t recognize them here. But that use without control by itself is not going to be a harm.

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

(Laughter.)

MR. CATE: It’s got accountability. It’s got risk management. It’s got FIPPs. It’s got consent use 72 times in it, and as a result, you can find anything you want in the GDPR and have no idea what your objective is in trying to comply with it. That’s why regulators in Europe are having so much trouble coming up with common standards for what to use. That’s why companies are spending billions of
dollars on lawyers, which I think is a great thing,
and I encourage you to do more of that.

(Laughter.)

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

MR. HO: Markus.

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

Since data privacy laws, data protection laws deal with the handling and use of data, it has to -- everything has to be looked at through the lens of how can we use data beneficially in a way that it
doesn’t hurt consumers? So these are actually two separate goals that always have to be kept in mind, and they should be explicitly stated in a privacy law. I believe the Brazilian privacy law actually says that right up front. There are two goals to privacy laws, protect privacy and enable the use of information.

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

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

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

That said, the compliance or governance
aspects of the GDPR which require risk assessments, as Markus mentioned and I discussed in the opening presentation, those do encourage, at least if not require, companies to think about things on a broader impact level. And that’s the part of the GDPR that is most of interest to me because it moves away from this notice and choice -- solely notice and choice regime to starting to think about the impact of data use more broadly on society as a whole.

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

In the US -- and this was a big issue in the invalidation of the safe harbor mechanism and remains an issue in the conversation about the Privacy Shield as mechanisms for transferring data from the EU to the United States. The question whether individuals can can have standing even under our existing sectoral privacy laws is hotly contested. And I think just as a broad-level observation, you see this strange
parallel of two minds set of jurisprudence arising at the Supreme Court where the standing doctrine on the one hand arguably seems to be moving towards really concrete, Scalia-style ideas of harm as measurable in terms of money, reputation, et cetera, where the Fourth Amendment jurisprudence of the United States increasingly looks at what we consider to be more big data or mosaic-theory-based and understandings of harm where you see in Carpenter, for example, or in Jones society-wide assessments of the possibility of a chilling effect from data misuse or from extreme collection, even in public spaces. And it seems to me that the Supreme Court has not yet put together those two prongs of jurisprudence to try to figure out how they interact with each other along the issues of what privacy harm actually is.

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

And Markus raised the question of protecting the individual versus enabling the use of information.
So query what privacy even means, but what mechanisms different models have to incentivize protecting consumer privacy. So, for example, are civil penalties a deterrent? That is an example of one mechanism, but there are myriad of others, and so I invite the panel to address that.

Yes, Shaundra.

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

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

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

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

MS. VANDRUFF: Markus?

MR. HEYDER: So, in addition to fines, as Shaundra mentioned and the other items she mentioned, I would, again, point to the concept of organizational
accountability, which requires organizations to implement comprehensive privacy management programs, which is essentially an ex ante exercise to prevent bad outcomes at some point and to avoid ex post enforcement. So that’s a huge ex ante mechanism to get companies up to speed in terms of protecting privacy.

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

And, finally, also from the GDPR, we can take the concept of data protection officer, or the DPO, which certain organizations have to have if they meet certain criteria, which also forces organizations to focus on privacy right from the start and to have somebody in charge and responsible and accountable for
implementing a comprehensive privacy management program.

MS. VANDRUFF: Margot?

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

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

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

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

MR. LEDUC: I mean, I think that really
underscores your point about this delicate balance but
a critical balance between regulation and kind of co-
regulation, right? I mean, we talked about that, and
it is hard to do, but we do have precedent for that
here in the US, and I think it’s a very, very strong
model going forward, I mean, the notion that we would
have a comprehensive federal privacy law and have it
be able to be enforced without some element of co-
regulation where we have public-private partnership
and the ability to help.

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

We can’t have this worked out through the
courts. We certainly don’t want it done through a
private right of action where, you know, we’re just
litigating it. That’s not the model. We do have a
model. And I think, you know, there have been
conscerns raised, frankly, about COPPA, which is, you
know, one of the best models that we have. And I
think some of those are fair concerns, frankly.

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

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

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

On the other hand, always a penalty is a failure. In other words, it means, the privacy has been violated, the harm’s been done, and now we’ve got
a penalty. So, really coming back to Markus’ point, the more we can do that tries to avoid that, that tries to create incentives for the better behavior up front, whether that’s safe harbors for certain types of behavior, whether that’s encouraging, you know, data review boards or other types of accountability tools, that the goal is to avoid the situation where we’re saying we got you for having done it wrong. What we want to do is have it not go wrong in the first place.

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

And the CCPA does this a little bit. CCPA does kind of create actually the requirements, I think -- someone correct me if I’m wrong here -- that the
state AG provide opinions to companies that are seeking opinions. Of course, one of the big problems is that it creates a bit of -- it creates in this instance a bit of a conflict sometimes for that agency and also I think creates this new obligation without establishing additional resources for the state AG’s office to carry out those responsibilities. But there is a recognition that there’s a role to play here for an entity to help translate the rules for companies that are trying to comply.

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

MS. KAMINSKI: Just one quick wrap-up, and apologies to Fred for having interrupted earlier. So, this idea that broad standards plus heavy fines is a recipe for corporate compliance disaster I do think runs really counter to how this is thought about in the EU. And not to pick sides on which form is right, but to the extent that we’re moving towards a federal privacy law that potentially preempts state privacy...
laws, it’s almost inevitable that we’re going to be moving to a vaguer standard as opposed to precise rules in that context.

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

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

MR. HO: Okay. So, I’d like to focus on the -- continue our focus on US laws. And David had mentioned COPPA earlier, and so here in the US, we have a number of privacy laws that cover conduct of entities that collect certain types of information, such as information about consumers’ finances or their health. Various statutes address personal health
data, financial information, children’s information, contents of communications, driver’s license data, viewing -- video viewing data, genetic data, and, you know, the list goes on and on.

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

MR. HEYDER: Yes.

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

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

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

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

And so -- and when we talk about this spectrum of information and whether it’s sensitive, you know, so our view of sensitive data is it would be
medical information, right? But even that health information that falls outside of HIPAA is still personal information that’s not protected by that sectoral law.

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

MR. CATE: And it’s not just gaps, it’s overlaps as well that are the huge problem. So why should it matter when I test my blood sugar whether I do it in -- using a medical device and it’s covered by HIPAA or I use my iPhone and it’s not covered by HIPAA, or I pay for my hospital bill and it’s covered by HIPAA but when the credit card charge goes through, it’s not covered by HIPAA.

This makes no sense to individuals who use data in a pretty seamless, global way around ourselves that all of these different laws abut or may not actually abut or in some cases actually overlap.

MR. HO: And Markus?

MR. HEYDER: Thanks. So I agree with
everything Shaundra and Fred just said. To the extent we need some sector-specific focus and expertise and more detailed elaboration around certain rules, I mean, I think we could draw, you know, from codes of conduct and certifications and use that mechanism to provide that kind of framework where it’s needed.

But otherwise I agree, we need a comprehensive baseline approach to privacy that covers all sectors pretty much equally.

MS. MOY: I do want to just highlight this problem that we are running into, though, that Shaundra was just touching on, that the distinction between information that we might have previously classified as sensitive and other information is rapidly disappearing if -- or, you know, or I shouldn’t say disappearing, but is becoming less of a clear distinction, right?

I mean, one can infer information about whether or not a person has Parkinson’s from sensors on the phone that might detect a tremor in a person’s hand, right? One can draw inferences about location of an individual from information about the individuals around them, right? From Mac addresses of nearby devices, information that we might not think of as historic -- as traditional location information.
Again, accelerometer and other phone sensor information, those can reveal information about -- not just about location but also about activities that an individual is participating in. And that’s one of the reasons that it’s important for us to focus not just on in the future protecting certain classes of information but also in ensuring that there are guidelines up that prevent information from being used, information about consumers from being used in ways that we find concerning.

So, if we would have found health information -- it concerning to use health information about an individual to target advertisements -- to target employment advertisements to that individual, then we might want to prevent other information about an individual that could be used to infer health information from being used to target those types of advertisements, right?

I mean, we might need to start thinking about how discrimination or other harmful data uses could flow from information that isn’t historically in the sensitive bucket and focus on preventing some of those uses.

MR. LEDUC: And that’s absolutely the focus of the NAI is to prevent certain types of data use for
advertising and to prohibit some of these sensitive
areas, but I think, you know, taking a step back, I’d
like to build onto the conversation talking about
personal information. I mean, we are at a -- at a
point where we’ve got this expansive definition
seemingly broader with every new bill in the CCPA.

I mean, I think a couple of people have
touched on that already today how it’s just so
incredibly broad to roll in everything. So and what
the impact of that is, unfortunately, I mean, I think
the previous panel, one of the previous panels where
Jules was talking about different types of de-
identification and use of pseudonymous data I think is
lost on a lot of policymakers today, the notion that
you can get good protection from certain types of --
around certain types of data, the use of pseudonymous
data that is not personally identifiable, identified
tied to a consumer that is applied and used with
certain controls, technical administrative controls,
legal controls, is a privacy gain. It’s a big privacy
benefit.

And it’s one that we are very proud to have
helped deliver in the advertising space, but this is
the type of thing that we need used throughout the
data ecosystem is we need to rely on this type of data
as much as possible. And we need laws that are going
to actually encourage that rather than discouraging it
by just creating a giant bucket and saying, well,
everything is personal data, everything is in the same
bucket and, therefore, you have to treat it absolutely
the same way. And it’s all very -- you know, clearly,
clearly, a lot of this data can be re-identified.
We’re long into the era of big data and
supercomputing, and we’re going to go further down
that path, but we need to be able to rely on certain
practices, privacy protection practices, rather than
just sweeping everything together.

MS. VANDRUFF: So, we’ve gotten a number of
interesting questions from our audience, and I want to
-- Jared and I would like to take an opportunity to
ask a few of them. And the first that I’d like to put
to our panel is about regulatory sandboxes. So, at
the outset, just what do you think about regulatory
sandboxes? But more granularly, is there precedent
for doing it? And how can it be done effectively
without giving companies a free pass?

MS. KAMINSKI: So this was a term or a
process that I was less familiar with before I spent
time in the EU. I think it’s interesting to think
about the notion of a regulatory sandbox in --
MS. VANDRUFF: And can I just interrupt you?

I’m sorry, Margot.

MS. KAMINSKI: Sure.

MS. VANDRUFF: Can you define for the audience what that means?

MS. KAMINSKI: Effectively a regulatory safe space for an industry -- a nascent industry to play in like my toddler --

(Laughter.)

MS. KAMINSKI: -- while it’s trying to figure out -- while the regulator is trying to figure out what the harms are and what the regulations should look like, so this is related to the concept of safe harbors but with a little bit more, I would say, proactivity on the part of the regulator in just deciding this is a space in which we want to sort of have a light touch.

And, again, I think the tension here is exactly again what Fred brought up earlier of you need to have vagueness in some ways, within the law for a regulator to be able to do that. You risk the possibility of capture if you do that. On the other hand, it does make the discussion of harms and concerns about an industry much more concrete than if you just full-stop employ a precautionary principle
and don’t let the industry operate and decide just to regulate it out of existence or alternatively more the US approach of not regulating it at all until you see concrete terrible harms impacting millions of people across the United States.

MR. CATE: I would just say I’m a huge believer in the regulatory sandbox, but we’ve been doing it for decades in the United States. It’s nothing new. For years, it was possible to come to events like this, you ask questions, you get responses. If you disclose something incredibly revealing, you know it could possibly be used, but on the other hand, it’s not generally the way that federal agencies go out looking for information.

And I think they’re also, to some extent, being oversold in some of the new environments in which they’re being developed, which is the same principle is going to apply there. If I go into the Information Commissioner in the United Kingdom and I disclose something that’s actually threatening to humans, I’m just guessing they’re not going to say, well, it was a sandbox, we don’t really care, we’ll just wait until we hear about it from somebody else. They’re going to say let’s follow up on that right now.
I think the point is that regulators serve multiple roles. And, again, the FTC has more exposure, more experience at this than anyone. And one of those is being able to participate in a dialogue where you get advice and the advice of others and you get feedback as opposed to just a subpoena telling you that now you’re in trouble.

MR. HO: Actually, so, we’re running short on time, and I want to give everyone their minute or two at the end to give their closing thoughts. So I’m just going to ask one more question that we received from the audience.

So we’ve been talking about the roles of state AGs when it comes to privacy enforcement, and as other states pass CCPA-like laws with added AG rulemaking, are state AGs the appropriate agency to provide rulemaking guidance and enforcement? Do we need something more akin to EU DPAs?

MR. LEDUC: Well, I mean, I think -- I don’t think we’re doing very well with the EU DPAs, or at least so far. I mean, I think that that’s the threat we face, right? I mean, whether it’s through -- I would think through -- mainly through a state model but certainly not a federal model to empower different decisions by different state ags.
I mean, I think it’s fair to say that no --
I mean, looking at a state legislative landscape and a
patchwork approach, no one is well served -- not
consumers, not businesses -- by having different
privacy -- you know, different standards in different
states. So I think we -- I mean, I think as a
practical matter, we can dispense with that.

Having AG enforcement, as I mentioned, is a
real, I think, benefit to the FTC, but in terms of
having rulemaking authority and the ability to, you
know, interpret the laws, frankly, if we were to kick
that to AGs just -- and let them all make decisions, I
think we would be back and we’d have just a disparate
set of decisions that would look a lot like if we had
a patchwork of different legislation.

MS. MOY: I just want to push back a little
bit on the idea that a patchwork is always bad because
I think that -- you now, I mean, from a consumer
perspective, a strong patchwork is better than a weak
federal standard, right? You know, so -- and if you
look at data security and breach notification, for
example, you know, we do kind of -- we have this
patchwork of state laws, if you will, and although
there are, of course, complaints about that -- it’s
not universally loved -- it offers a lot of benefits
Between 2015 and 2018, I think 23 states updated their data security and breach notification laws. That’s a lot of activity. A lot of those updates happen because state AGs have contact directly with both companies and consumers, see a shifting landscape and make recommendations to the state legislature that it respond to shifting threats. So one of the big things that happened is that a lot of states updated their laws to cover health information, not just health information collected by healthcare providers but maintained by other types of entities as medical identity theft was on the rise. So there is sort of this -- there’s this legislative agility function that having state legislatures and, if you will a patchwork of state laws, that does serve consumers in many ways.

MS. WATSON: I think I would just add, though, just the premise, I think we want to see a strong federal law, and so I wouldn’t assume away the fact that a federal law would be weak. I think we think of sort of replacing state laws is appropriate if we are able to craft a robust and strong federal law.

And the other thing is on a data breach
notification piece, that’s obviously been a significant challenge for businesses. But I think that problem is magnified when you talk about sort of these broader privacy issues when you’re going to the heart of the architecture and what companies are doing and how they share data. And so I think that’s a little bit of a different animal than this piece of notification because the coverage is so broad and the impact is so significant.

And so I do think that the different and conflicting obligations would present a significant challenge, and it’s not just about sort of what companies -- the obligations that they provide, it’s also what consumers expect. And so I just think a better approach is to have one national standard that provides clear expectations for consumers and clear obligations for businesses, but you know, I do agree that that should be in the form of a strong federal law, not a weak one.

MS. VANDRUFF: So, Shaundra, you’ve given me the perfect opportunity to ask --

(Laughter.)

MS. VANDRUFF: -- our last question of the panel, which is, you know, we talked over the course of this hour-plus about different frameworks and what
different bodies have done to tackle privacy.

I guess the question is, you know, what -- if we were to take different parts from different privacy frameworks that we’ve been discussing today and that you all have studied in your academic work and in the course of representing your various clients, what should a federal privacy framework look like? What part of existing law such as the CCPA or GDPR or other state law should we use as guideposts? And I’d ask each of you to just take a minute or so to address that question. And, Shaundra, you started, so you get the first swing at this.

MS. WATSON: Sure, sure. So our member companies think a federal privacy law should include three key components. The first is to give consumers the right to know and the right to control what happens to their personal information. The second is to impose obligations on companies to safeguard consumer data and to prevent its misuse. And, finally, we believe there should be strong, consistent, and effective enforcement.

MS. MOY: So I’ll say -- so I think a couple things that I would take from GDPR are data minimization and purpose limitation and powerful fining authority from CCPA. I probably would take
state AG enforcements, but then I also think that it’s really important that we see rulemaking authority to ensure fairness in automated decision-making and to prevent things like discriminatory advertising, not just eligibility determinations but advertising of opportunities. And a private right of action in no small part because historically disadvantaged communities have not historically always been protected by agencies when agencies are expected to protect everyone.

MR. LEDUC: Well, as some of you may have heard, we formed a coalition yesterday and announced an effort to promote legislation, and it echoes -- you know, what I’ve said today really echoes that movement, and it’s really largely focused on the notion of enforcing around reasonable and unreasonable data practices, picking up on what Laura said, creating clear categories and uses that are unreasonable and those that are reasonable and building in an opportunity for co-regulation, expanding the authority, expanding the resources of the FTC and giving them some -- I mean, I think some appropriate authority, creating a new bureau of data protection to be able to enforce around this notion of what is unreasonable.
I mean, I think the FTC did some really good work over the last couple years under acting Chairman Ohlhausen, really assessing informational injuries. And I think we could all define them differently. I think we can all agree they’re nearly impossible to clearly define, but we need to protect against those practices, those bad practices. So a framework that can really help us do that and let us be able to use data for good purposes, promote innovation, and continue doing things that consumers want.

MR. HEYDER: So we need a comprehensive baseline privacy law. We think it should be based on the concept of organizational accountability. It should take the risk-based approach. It should employ codes and certifications to outsource, so to speak, some of the functions that otherwise would belong to the FTC. There should be strong enforcement powers by the FTC.

I think, ultimately, we should use the accountability model to move away from the situation that was discussed in the earlier panel where everything’s about consumer expectations, secondary uses that you can pick and choose from and where you control everything that happens to your data. Instead, we want to create a system where every
organization that touches data is sort of tied into this organization -- accountability framework that is enforced against them and that enables consumers not to worry about secondary uses that are otherwise beneficial for society and for themselves.

And for organizations that are implementing accountability to focus on risks and harms and to have an obligation to prevent those. So to free up consumers from having to be engaged every day, every single day on what happens with the data and what doesn’t happen. There’s a place for consent and for making choices, and I fully agree with some of the examples that were given, but for the most part, as Fred had suggested earlier, that’s no longer possible and feasible.

Finally, a US policy framework should be interoperable as much as possible with other frameworks like the GDPR for consistency purposes to -- that would benefit companies in terms of implementation. It would help regulators in terms of enforcement and would help consumers in terms of providing consistency across the globe.

But this interoperability or alignment with other models should not come at the expense of 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
5 MR. CATE: I feel sort of lonely up here.
6 Everybody has a "we" that they speak for. And I don’t
7 know, Margot, do you? Margot and I just speak for all
8 rational people everywhere --
9 (Laughter.)
10
11 MR. CATE: -- and we think -- I think there
12 are really six elements that should be key here and
13 one is put consent back in a box. It should not be
14 the dominant focus. It’s not rational. It’s not
15 usable. It’s not workable. And it’s frankly not fair
16 to individuals to say that we’re going to be held
17 responsible for the effects of decisions we may not
18 even know we’re making, even though we can’t possibly
19 understand what those effects are going to be.
20
21 Two, I would focus a lot less than US law
22 has historically done and certainly than European law
23 does on collection and much more on use. What we’ve
24 learned, especially in the area of government
25 collection of data, there’s always a legitimate reason
26 to collect it. There is always a legitimate use. You
27 need it for a credit card transaction. You need it
28 for online. You need it for dealing with a doctor.
You need it someplace.

And what we don’t want to limit our focus on is the terms under which it’s being collected but rather what is it being used for and, more importantly, what is it being reused for and how is it being used in ways that may be shocking or potentially harmful.

Third, accountability, which I think Markus has been eloquent on, but again the notion of responsible stewardship of data and that we expect organizations that collect and use data to do so in a way that is responsible and that they will be accountable when those data cause harm.

That suggests the fourth, which is what the Europeans call a risk assessment model, but basically a harm-based model, that that should be the focus. We’re not trying to nail down everything. We’re trying, like most consumer protection laws, to prevent harms that can be prevented. And there’s a lot that we agree are harms, and then that leaves an area where folks can rationally disagree and courts might play a role.

Fifth, vigorous federal enforcement and a federal regulator. I personally think that should be the Federal Trade Commission, but it would mean a lot
more staff, and it would clearly mean rulemaking authority. It’s not sufficient to say after the fact what’s been done wrong.

And, finally, remembering what I’m now going to call the Heyder Principle, and that is on the other side of this balance are the extraordinary benefits we get from the widespread use of information. And they’re important economically. They’re important personally. They’re a foundation of a good part of the 21st century economy, and people love those benefits and expect those benefits, and so we should keep in mind this is a balance at all times. It is not a single focus issue.

MS. KAMINSKI: I have 17 seconds to say my concluding thoughts on this. And I think that largely we’ll be agreeing on a lot of the high principles and disagreeing on some of the probably most important decisions. And those things that are the focus of most disagreement include both the issue of preemption and the issue of private rights of action.

The second sort of substantive category I would add in there -- we didn’t get time to talk about today -- but where I agree that focusing only on notice and choice is a very limited way of looking at privacy and, in fact, in practice has been
individually disempowering. There are elements of individual empowerment that I think are important, and principles about data collection that are also important that exist in the EU regime and don’t exist here.

So in the CCPA, we don’t really see, as I said, much in the way of purpose limitation, purpose specification, and use limitation principles. We don’t see data minimization principles, and the use case I’d like is to try to think through a little bit when we’re trying to find points of disagreement rather than agreement is the idea of monitoring of biometric information in public spaces. I think that teases out a lot of the divides potentially in these communities.

Very last, I promise, we’ve long seen a hybrid state/federal regime where we can conceive of data privacy, or I guess privacy more generally as being simultaneously a global federal issue and a highly localized issue. And as we move to a world of smart cities and CCTV-monitored public spaces, states and even municipalities really do see those concerns as being issues that are subject to their purview and even local police powers. Thank you.

MR. HO: And thank you. Please give our
panelists a round of applause.

(Applause.)

MR. HO: And with that, we’ll start our break. And please return promptly at 3:45.

(Recess.)
CURRENT APPROACHES TO PRIVACY, PART 2

MS. JILLSON: Welcome back, and if you would all just take your seats, we have one more panel discussion this afternoon.

So before the break, we had the first part of the current approaches to privacy, and for our last panel discussion today, we have Current Approaches to Privacy, Part 2. And what we will be doing is trying to take some of the broad principles that we talked about before the break and make this a little bit more concrete. So we’re going to be walking through five hypothetical scenarios in which these panelists are going to be trying to tackle specific problems and try to unpack how would CCPA deal with this problem, how would GDPR, how would the US sector-specific approach.

But before we get into the substance of that, let me take just a moment to introduce myself, my comoderator, and our esteemed panelists today. My name is Elisa Jillson. I am an attorney in the Division of Privacy and Identity Protection. My comoderator is Andy Arias, also an attorney in the Privacy Division.

And here today, we have Lothar Determann, who is a Partner at Baker McKenzie; Jay Edelson, who is the Founder and CEO of Edelson PC; Rebecca S.
Engrav is a Partner at Perkins Coie; Alan Raul is a Partner at Sidley Austin, LLP; and Tracy Shapiro is a Partner at DLA Piper.

And so how we’re going to start off with our panel today is Lothar is going to tackle our first hypothetical. He’s going to take a few extra minutes to kind of lay some groundwork on some of the key differences between CCPA, GDPR, and other laws. After he takes that first crack at the hypothetical, we’ll open it up for discussion with the rest of the panelists, and then we’ll be moving along to the next hypothetical.

So with all of that said, I’ll hand over the clicker to Lothar, and thank you very much for taking us to the very first hypothetical. And I’m sorry, if you could click the slide one forward, I’ll just read the hypo, and then we’ll get started.

So Company A, a US startup with a German subsidiary, offers a newsletter for cycling enthusiasts with information on safety, health, and new cycling products. It’s funded through ads. It is developing a new product that can sense danger, such as weather changes or drunk drivers, and warn cyclists. Health insurance companies, automakers, and city planners seek access to its data.
One day, an engineer inadvertently accesses a file containing name and health insurance provider for 200,000 employees and newsletter subscribers. Lothar, what are the implications for this company’s practices under various legal regimes? Please walk us through that.

MR. DETERMANN: I will walk you through, and I’ll lay the groundwork, too, that you invited me to lay. Thank you so much for inviting me. It’s wonderful to be in DC, particularly at cherry blossom time. And I agree with Commissioner Phillips wholeheartedly that it was a fantastic set of panelists today, and I very much enjoyed this today and tomorrow, what I’ve heard, and I’ll try to lay a little bit of this groundwork and apply the insights and the broad principles and the purposes of different approaches to privacy law for our panel, which is now going to apply this to concrete hypotheticals.

The current approaches to privacy law vary from country to country based on different needs and preferences of people or governments, for information, for human dignity, security, privacy, freedom, and technological innovation. Let’s start with Europe, the old country. We heard to protect privacy and prevent George Orville’s vision of 1984, the European...
countries regulated data processing as such, with a prohibitive and bureaucratic regime.

European countries prohibited data processing by default. And companies and governments must not collect, use, share personal data except as specifically permitted. The basic idea was the less we use computers and data, the better for data privacy. This is from the 1970s. This was harmonized in 1995. The question was raised what the purpose was. It was a trade measure to enable free flow of information within Europe and cut off flow to other countries. That was the ‘95 directive, and that idea of the free flow of information in Europe for economic development is still in the GDPR.

So what happened through the ‘70s, European citizens embraced information technologies made in the US, increasingly in Asia, the same compromise on privacies elsewhere. Where the European governments were constrained by data protection laws and intelligence gathering, foreign governments, including the US NSA, stepped in. And where the European companies were hindered in developing information technology products by this data processing regulations, US companies stepped in.

Effective May 2018, the EU GDPR doubles down
on this approach of the ‘70s with even more
prohibitive data processing regulation and large fines
that are intended for US tech companies specifically
as publicly stated. Additionally, the German
Government came up with creating property rights in
mobility data to protect the local auto industry from
competition, which underlines that one of the purposes
of privacy and data protection law is also trade.

Now, we already heard about the US approach,
very different path. Data processing, as such, is
allowed and we have focused on harm sector situations,
specific privacy laws that are constantly updated,
supplemented, and are actually enforced, which has not
been true in Europe for much of the 50 years of
history there.

We have in California the first data
security breach notification law worldwide, 2002. It
took the Europeans 16 years to follow this. We had
the first law requiring privacy notices for websites,
2004. We have dozens of other privacy laws. We have
one for supermarket club cards. We have one for RFID
tax. We have one for automated license plate
scanners, and that’s important to understand when CCPA
is sold as an omnibus law, it’s just one of literally
dozens of laws in California, alone in one state of
the United States.
I believe these laws have effectively
protected individual privacy against newly emerging
threats while allowing technology to thrive. And the
FTC has done its part in developing a body of data
privacy and security law that is focused on preventing
consumer harm, but after enacting laws for 50 years,
situation-specific, and without repealing,
harmonizing, or updating the existing laws and
streamlining them, simplifying them, the US are now
also suffocating innovation and business.
The California Consumer Privacy Act against
data sharing overburdens companies with excessive,
complex, rigid, and prescriptive requirements. If
other states follow and Congress does not preempt,
only the largest of companies will be able to handle
compliance.
Now, let’s look at Asia a little bit, too.
I’m at the West Coast. We don’t just look to Europe.
The Asian countries strongly encourage and support
data-driven innovation. The People’s Republic of
China focuses its data laws not on individual privacy
but on data residency requirement, internet
censorship, and protecting Chinese-owned companies
against foreign competition.
China mandates Chinese companies to develop and apply artificial intelligence, big data analysis, social scoring, and we see other countries taking their own path. India is following a hybrid approach combining the Chinese and Russian data residency requirements with European data processing regulation, but most of the other countries are more or less following the European data processing regulation approach, at least on paper.

If the United States also follows the European approach and regulates data processing with GDPR-like law, established multinationals will appreciate and benefit from international harmonization for sure, but startup companies will be hampered and innovation will slow. This will hinder progress in autonomous vehicles, artificial intelligence, and, as we heard on one of the previous panels, in the healthcare sector. I believe it will be literally unhealthy.

If the United States follows Europe or stays on its current course and fails to streamline and harmonize its myriad privacy laws, I expect that global innovation leadership will move to Asia. In a few years, US citizens will then be using technologies made by Chinese companies, and the impact on
individual privacy, national security, and the economy in the United States would be similar as in Europe since the ‘70s, and in that sense I think we should and can learn from the European approach, which will now apply to our hypotheticals.

We start with the hypothetical that Elisa just read and take a look at the benefits that this company offers to consumers and the risks to privacy. The benefits include global, local information free of charge for cyclists. I’m a cyclist enthusiast. I appreciate this greatly. And it is developing life-saving new cycling safety technologies, which are very much needed. As healthy as cycling is a danger it is. And it offers attractive jobs in the technology sector.

Now, there are risks. They include, as we heard the previous panel and the first panel today and also in the ninth session December 12 from Professor Solove, discrimination by employers, insurance companies based on habits, health condition is embarrassment, fraud, stalking, and many other harms that we should definitely take into account.

Now, how do these different approaches to privacy now have an impact on this company in our hypothetical? The EU GDPR does not, contrary to
common belief and as often emphasized as an opt-in law, would not require this company or its German subsidiary to obtain consent from consumers. European companies can and often must rely on alternative means of justifying the data processing against this general prohibition of data processing and rely on things like necessity-performed contracts or legitimate interests that are not outweighed by the overriding interests of the data subjects.

The GDPR, as broad as the prohibitions are, as broad and vague are some of the exceptions, but the GDPR also puts a lot of paperwork obligations and data minimization on our company. It asks the issue of very specific notices that are different and have different requirements. They’re not really compatible with the kind of notices that the FTC requires, which have to be understandable by consumers, not possible with the details required for 12 to 13 GDPR.

They have to satisfy data access portability deletion requests free of charge to individuals but to the public and community appointment of a data protection officer, designation of a local representative for the US company, data protection impact assessments, documentation to demonstrate. It goes on and on, particularly also to satisfy the
international transfer restrictions that are specifically benefitting the European companies and to the disadvantage of foreign companies.

Compliance is very expensive for the startup company, and these requirements are not focused on any particular harm as was noticed on the previous panel. The privacy harms are not core and center. It just discourages data collection on this idea the less data collected the better for data privacy.

Now, the CCPA does its own part here. It doesn’t prohibit anything. There’s no data minimization in there. But the CCPA will require, in conjunction with other California laws, very specific and elaborate disclosures that are not compatible with other US laws or the GDPR. Companies, if they want to share data with other companies in certain circumstances, have to put a special link on their website that says “your California privacy rights.” They have to put a link under the CCPA for do not sell my personal information, and if every state in the US and every country does that, then all the websites and the mobile pages of the world will be full and we won’t put any other content on them.

Also, the California residents may opt out of information selling but remain entitled to service,
which we heard on a previous panel will cause
companies to start charging for services that are now
available for free, which will take one important
consumer benefit away.

Residency requirements in countries such as
Russia, China -- in India the bill is pending.
Indonesia and Kazakhstan will require our startup
company to establish a local presence to keep all data
there so it’s accessible to the local government,
which startup companies often can’t afford to do.
Plus, in China, a company that is not Chinese-owned
can’t do much over the internet anyhow under the
regulatory regimes.

Perhaps the biggest impact for our company
that wants to develop this safety device, though --
and this one is not about advertising as pretty much
all previous panels were focused on -- is to develop
the sensors and train the self-learning algorithms
they need to collect data on public places, on public
roads. They don’t need identifying information, but
they need data on what a person looks like, sounds,
smells, acts, and so on.

And this is personal data under European
law, personal information under the CCPA, and
companies should be able to exchange this information
with other companies, otherwise, every single company
has to drive around everywhere to collect this
information. But the GDPR makes this extremely
difficult and nearly impossible for a company in
another country due to the restrictions on special
congratulations of personal data. You have to get
consent for transfer to the US, which is impossible.
You can’t drive around on the street and then get
parental consent inviting from a kid that happens to
be on the camera.

Similar, the CCPA requires opt-in consent
from teenagers and also parental consent for minors,
which is just not practical. So these technologies
will not be developed with input in California, with
data from California. In China, the activities are
encouraged by the government for Chinese companies.

Now, the second part of our hypothetical is
one that illustrates a slightly different point.
That’s the data security breach. And we heard on the
previous panel what a hard time companies have when
they’re faced with such a situation. I think the
practitioners on the panel will agree. You have to
look at 50 different state laws, plus different
countries’ laws, to determine who you have to notify
in Europe, in what language, what regulator has to be
notified in 72 hours. And that adds a huge compliance burden.

Plus, on top of it, if this list with just people’s name and the name of their health insurance company is law, then everyone on that list is entitled to between $100 and $750 statutory damages under the California law without any showing of harm.

With this hypothetical, I mean to illustrate just a few points, namely, that the broad prohibitions on data processing and also data minimization cause too much collateral damage and don’t do enough for privacy. The data genie is out of the bottle. The data is everywhere. We need to focus on the harm that it causes and specifically legislate that.

As we heard on the previous panel, if discrimination is the problem, then we need to prohibit that form of discrimination and act on it and enforce and not just prohibit every data sharing and collection.

The data processing regulations in Europe have been largely ineffective. The GDPR is not a modern law. It’s 50 years old. It’s doubling down. And similar threats follow from the excessively prescriptive and complex disclosure requirements and data subject rights like the CCPA, particularly since...
that is one law for 50 states.

Diverging disclosure breach notifications
and other requirements on the state level hamper
interstate commerce, should be harmonized nationwide,
and I personally believe the United States and the FTC
have been on the right track to focus on consumer harm
and individual privacy, but they do need to now
streamline and harmonize existing laws so that
organizations, particularly smaller businesses, can
realistically understand and comply with privacy laws.
Otherwise, these laws will be counterproductive if
nobody can follow them anymore.

I’m looking very much forward to our
discussion after this little bit of groundwork.

MS. ARIAS: Lothar, thank you very much for
that. So let me open it up to the rest of the
panelists. Lothar did a very good job of kind of
detailing some of the issues with this hypothetical,
but I’m curious if you all have any other thoughts
about maybe some of the issues that he may not have
been able to cover that kind of pop into your minds.

MR. EDELSON: Yeah, I’d be happy to jump in.

MS. ARIAS: Jay, please.

MR. EDELSON: So I come at this from a
totally different perspective. I’m on the plaintiff
side. I represent class actions and also regulators at the state, city, and county level. The first thing, it was interesting to hear that if we have strong privacy laws, then it’s going to stifle innovation and everything’s going to go to China. I think that that -- that’s really not going to happen.

Let’s focus on what most privacy laws are, and those are consent laws. And that really for me, the focus of the hypothetical has to start with that, which is did Company A, did the startup get consent? And it’s really not hard to do. That’s why I don’t think it’s a huge burden. It’s not going to stifle innovation. All they have to do is say, “Here’s what we’re collecting, and here’s what we’re going to do with it.”

Now, an issue which was brought up and it also was brought up in previous panels was we’ve got all these different laws -- there’s federal -- I’m going to focus on American law, the one thing that I know about. I’ll leave the EU to you. This idea that if we have differing laws, we’re all going to just -- it’s too much to handle. First, for data breach notification, I think it proves the opposite. We’ve seen that companies have no problem complying with the myriad data breach notification laws. Although, I
agree, having a uniform law there might be helpful.

With regard, though, to laws more generally, if you look at what plaintiffs -- whether they be regulators or private citizens -- sue under, they generally start with consumer fraud statutes. So the FTC will look under Section 5 of the FTC act. You’ll see state attorneys general will look at consumer fraud statutes. When there are damages -- and can get into what it means to be damaged -- private litigants will look at consumer fraud statutes there.

And, again, the big issue is let’s look at what the public-facing statements are and compare them to what actually is happening. And if there’s a mismatch, then that’s when the company ought to be held accountable.

MS. ARIAS: Anybody else on the panel have any additional thoughts?

MS. ENGRAV: Just a small point. I think I heard you correctly to state that in -- for the breach part of the hypo that you would see a -- that this would -- this would trigger under the CCPA and potentially at the private right of action. And, of course, none of this has been litigated yet. But there is some language in that that I think might make it such that, set aside for the moment whether it’s a
reportable incident under existing California law,
that the private right of action wouldn’t apply there
because some of the additional language there is
whether it’s subject to unauthorized access and
exfiltration, theft, or disclosure as a result of the
business’ violation of the duty to implement and
maintain reasonable security procedures and practices.

So I think maybe we just don’t know yet. I
think we’d need to know more facts about this fact
pattern. How inadvertent was it? Were there good
procedures and practices in place? And so I think,
like, there just might be a little bit more going on
to that question.

MS. SHAPIRO: I would add the same thing
with regard to the health insurance question, that if
they start selling information to health insurance
companies, we’d want to know more, like, are they
advertising that as a purpose for the use? Are they
marketing the data? And in that way is there a Spokeo
situation? Is there a risk that they become a
consumer reporting agency because they’re marketing
the data for purposes of making eligibility
determinations.

MS. ARIAS: Thank you. Okay, since our time
is short and we want to cover all the hypos -- we have
fiver hypos for you all -- we’re going to go ahead and cut the discussion here and move on to the next hypothetical.

MS. JILLSON: So hypo two, Company B develops a free mobile app with a location sharing opt-in that offers shopping discounts based on location. City planners interested in making downtown shopping areas more “walkable” offer to pay for access to the app’s data.

And, Rebecca, perhaps you can start us off with this hypo.

MS. ENGRAV: Sure. So I think for me it’s helpful to kind of take it into really concrete questions in terms of is this okay or is it maybe okay, depending on different facts. And I think it’s important to keep in mind that the hypo itself gives us the concrete fact that the original location sharing is opt-in. So we can all just assume that. We don’t have people who don’t know that the location data is being collected and they had a choice. It was opt-in.

So as to the second part of it, though, about can Company B share it with the city planners when they offer to buy this data to kind of help solve 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
to consumers. So there wouldn’t be an existing
deception issue.

10 If we assume that, then under US laws that
11 exist right now, in my view, kind of Section 5, the
12 state UDAP laws, there’s no special law applicable to
13 this company. It’s not in a regulated sector. So
14 there’s no particular opt-in or opt-out requirement.
15 We’re just in the land of general consumer protection,
16 be honest and accurate in how you describe your
17 product, and if you’re not -- if this isn’t at odds
18 with anything that they’ve said, I don’t think there’s
19 any particular opt-in or opt-out requirement.

20 If we then shift to CCPA, that’s a more
21 interesting question there. CCPA, of course, does
22 have disclosure and opt-out -- not opt-in, but opt-out
23 -- required for sharing of data with a third party
when it’s a sale. And here, the hypo is telling us
that it would be a sale because the city planners are
offering to pay for it. So if that’s all that’s going
on under the CCPA analysis, then consumers would have
a right, both to be specifically informed about this
and opt out of it.

I do think under the CCPA there is a
question that would come up about the fact that this
is a city getting the data. There are several
provisions in the CCPA that speak either to different
levels of law or to kind of just different aspects of
how governments might or might not either fall within
this, and here they’re not even the subject, they’re
the third party.

So I certainly haven’t thought all that
through. I don’t have an answer for you, but I can
definitely say in my look through CCPA preparing for
this I’m highlighting a lot of provisions that talk
about government and different aspects of levels of
law. And I think that there very well could be a
different answer under the CCPA for data sharing with
governments, as opposed to data sharing with other
private companies, even it’s a paid exchange. And I’m
curious, actually, if others on the panel see the same
issue there.
But just to kind of close it out here on the front-end question of do you need opt-in consent for this, from a GDPR perspective, it’s interesting, I think we tend to think, oh, the GDPR is so protective. EU is so much more conservative. You know, interestingly, there’s, again, no opt-in or opt-out specific requirement here unless the company were planning to rely on consent, which it likely wouldn’t because it’s very rare to rely on consent because of how onerous that standard is in the EU, they presumably would be relying on a different legitimate interest.

So long as you have a legitimate interest, your obligations to provide transparency about what that basis for processing is, but there isn’t a specific sort of opt-in or opt-out requirement. So if -- so we’ve worked all that through. The company’s decided that, yes, they can share. They’ve checked their disclosures. They know their privacy policy, kind of it’s great. It already says we share with third parties.

A next kind of threshold gating question to think about, I think, would be does it matter how many subscribers this app has? And there we also do see a little bit of a distinction from the CCPA, and there
are some really real practical questions for companies about those triggering thresholds under the CCPA. There’s three of them. Do you have 50,000 California residents? Or gross revenues in excess of $25 million? Or at least 50 percent of your annual revenue by selling the personal information of California residents?

So this business, again, we don’t know enough facts, but depending on if they’re based in California, if this particular form of data sharing and the money they earn from it is really their only source of revenue, and/or it’s a small app, so they definitely don’t have 25 million in revenue. I’m making that up. So they may or may not come within a CCPA-type law if there are these thresholds to it.

The existing federal regime, of course, doesn’t have any particular thresholds. GDPR also doesn’t have any particular thresholds. But that could be another way where the regimes differ in how they treat it. This app, interestingly, some apps are going to have a real challenge figuring out where their residents are located in terms of deciding which ones they’re going to decide, are entitled to CCPA-type rights.

You know, that’s a great benefit, actually,
of online services. And if you’re doing a good job of
following your privacy principles of data minimization
and not collecting data you don’t have, an app like
this may very well have user name and email address.
I mean, it’s a pretty thin, simple app. So unless
they’re just going to draw inferences from IP address,
they’re not necessarily going to know where their
residents are located, unless they try to backtrack
from their location, collecting portion and saying
that anybody who walks in, you know, Menlo Park is a
resident of California. Visitors from Illinois, I
don’t know how that would work out.

So I think the third piece that I’ll talk
about then before we open it up to the panel is to
think about, well, what if the city has a breach. So
the city’s received this data, kind of worked through
all the steps and, you know, the Company B was fine
sharing it. But the city doesn’t have great data
security. They have a lot of turnover. Every time
there’s a new administration, this is just a file
sitting around, and they have a breach. What happens
then?

Under existing law, location information
alone wouldn’t trigger breach reporting in the United
States. In Europe, it might. The standard there
would be a substantial risk to the substantial rights
and freedoms of the data subject. And if you have a
lot of location information -- we also don’t know from
this hypo if the city planner is seeing each of these
data points as just individual data points or if the
city planner knows that it’s Person A making all of
those data points. We can’t tell that from this. But
that distinction may make a difference to your
European breach reporting obligation there as well.

But as to who does the breach reporting,
that would also be an interesting question here if
it’s a city planner breach. We’ve got kind of
existing, you know, that happens in the United States.
We already have plenty of fact patterns of where a
downstream vendor, a service provider encounters a
breach. They need to tell the first party from whom
they got the data, but it’s the first party that would
conduct the breach reporting. Here, there could be
some interesting questions, depending on what time the
breaches happened in terms of ability to find the
folks and provide notifications.

MS. JILLSON: Well, thank you, Rebecca.
That’s a great job spotting some tricky issues. We’ve
gotten an interesting question from our audience. If
the app says “we collect location information to
provide you discounts,” is it a deceptive failure to disclose under Section 5?

MS. SHAPIRO: I’ll jump in on that. So I think it’s a very challenging question, and a lot of my clients debate this issue with looking at the Golden Shores case that the FTC brought, where there was a flashlight app. They were collecting geolocation information. There, they didn’t say that they were collecting it or sharing it, and there was nothing in the privacy policy.

So I think there is this question of, okay, if we’re not that severe, and the consumer expectations were such that you would never think that your flashlight app is collecting location, but let’s say you’ve got an app where it is expected that location would be collected, like here, it’s clearly disclosed that it is, do you need to have that sharing in just-in-time disclosure, or can it be in the privacy policy?

You know, the FTC has certainly said we want it to be an opt-in for the sharing of location data, and we want it to be just in time. But it was a consent order. It’s not binding law. But, you know, do you want to be the company that tests that by not following the Golden Shores order?
MR. RAUL: And I would add if this is taking place in California, and with all the walking and cycling going on and the CCPA, I'm sure everything is taking place in California, there might be a CalOPPA, the statute in California that requires privacy policy disclosure for online collections of personal information about California residents. And if that doesn't include a disclosure of selling to the city, there might be an issue there.

Another kind of off-the-wall issue here, you know, we're kind of brainstorming here and free association, is this is a city. Is surveillance involved? And that's an issue that might be of concern to people. And is the stored communications act involved where if -- if they're a communications provider, this app, which is sometimes an ambiguous category, they would require, in order to provide the information to a government agency, some kind of legal process, like a subpoena, unless, of course, it were with the consent of the walkers here.

One last comment is the ambiguity in California for opt-in versus do not sell. So what if they -- the people who are using this app opted in specifically to all kinds of stuff, and then, you know, California CCPA goes into effect, and they're
pushing "do not sell" buttons all over the place. Did they really mean that? Did they really mean to omnibus, don’t sell when they want all these discount coupons? So you know, we’ll see how that -- how that plays out.

MR. DETERMANN: Just on that last point, I think the CCPA is pretty clear that people could opt out then and then companies can’t ask them to opt back in for a year if they made a mistake. When I looked at this hypothetical, I was going to say to my client, you know the discount model you can do without data sharing because the consumers will go and show the discount, and that’s how the merchants see that this is in effect and that’s how they’ll pay you. But the city planners get no more data from you because that would trigger the “do not sell my information” link on the mobile app that causes a lot of hassle.

And at the Smart Cities conference in Stanford, the city planners had already complained that they’re not getting personal data or any data from the private sector anymore with these privacy laws becoming more and more burdensome on companies who want to share for public purposes because any benefit under the CCPA will count as selling. So even if there was some other leniency or some benefit that
the city would offer instead of cash, it’s selling, it would trigger the link, and many companies don’t want that ugly link on their sites, and they will just stop sharing data. That will be the impact of the CCPA, I think, on this hypothetical.

MS. JILLSON: Well, in the interest of time, let’s move on to the next hypothetical.

MS. ARIAS: Though I think Lothar’s statements are actually pretty timely about the "do not sell my personal information" because this hypo is going to cover a little bit of that.

All right. So Company C sells fertility trackers in which users can record the dates of sexual activity and diagnosis or treatment for an STD. Company C decides to provide access to de-identify data sets to pharmaceutical companies, public health advocates, and advertisers.

Carla Consumer doesn’t want her personal information to be sold. Frustrated that she can’t find a "do not sell my personal information" link, she deletes the app. A year later, Carla asks Company C to delete all information about her.

Tracy, can we talk a little bit about the privacy implications of this scenario?

MS. SHAPIRO: Sure. So, you know, first, I
would think about the legal framework here and what
laws might apply. So, you know, whenever there’s
health data, my first question is always is there a
HIPAA issue? There’s no mention to the fertility
tracker being a covered entity that gets reimbursed or
electronically bills insurance providers. It doesn’t
sound like it’s a service provider to fertility
doctors. So there’s probably no business associate,
BAA, kind of governing the use of the data.

But, of course, not being covered by HIPAA
doesn’t mean that you’re not regulated. The FTC, as
I’m sure everybody knows, has made clear that they
view health data as being sensitive information. And
I’m sure they would consider STD and sexual activity-
related information to be sensitive. So you’ve got to
think about the implications there with regard to data
use and data sharing.

I would be thinking about the NAI guidelines
that says they’re sharing with advertisers, unclear if
there’s OBA going on, but the NAI speaks to the use of
sensitive information, including STD-related
information for targeted advertising and the need to
get an opt-in.

I’d be thinking about CCPA, which doesn’t
specifically address health information but talks
about data sharing and places restrictions there. I think about CalOPPA and transparency requirements and then, of course, GDPR and considering whether you’ve got a legal basis for processing this data.

So with that framework, I think there are a few big issues that jump out at me in the hypo. One, there’s the sharing of de-identified data with these three entities. And it sounds like it’s a new use of sharing. So it says that Company C decides to do this, which suggests it might be a change in its practices. So with the de-identification, I would be thinking about does this de-identification practice that Company C implements, does it comply with the various standards for de-identification?

So with CCPA, we’ve got a super broad definition of personal information and a really broad and quite circular definition of de-identification. So I think a lot of us are struggling to figure out exactly what -- how one can actually de-identify data at this point under that law. It also requires that one puts in place technical and business processes to prevent the de-identification of data. So we’d need -- Company C would have it look at its contracts that it’s got in place with these recipient entities.

If Carla’s not in California, I’d also be
thinking about FTC guidance. On earlier panels, they talked a lot about the de-identification standards that are set forth in the FTC Privacy Report. You’d also need attestations by the recipients that they won’t make efforts to re-identify the data. And then if she’s in the EU, I would be thinking about GDPR, which also has an incredibly high bar for anonymization, and most likely Company C won’t be meeting that standard in disclosing the data.

So then we’ve also got this change in the treatment of data. You know, it is a very basic and long-standing FTC principle that if you have a material change to retroactively collected information, the FTC wants you to get opt-in consent for that. So you’d have to consider here is this a material change in the treatment of information. I’d want to be looking at what Company C told users in the privacy policy with regard to how they share data. It could be that they had a super broad disclosure that would maybe cover this. But if not, they’d want to be thinking about whether they need to get an opt-in consent for that.

I think about CalOPPA, which says in your privacy policy you’ve got to say how you’re going to notify your users of material changes, so you’d want
to make sure whatever method you set forth there
you’re complying with that. And then, of course, with
GDPR, you’d want to be thinking do you also need to
get consent for these disclosures.

And then two other considerations. So we’ve
got Carla wanting to opt out. She doesn’t want her
personal information to be sold, and she’s frustrated.
So, you know, one, if I were Company C, I’d want to be
thinking about if she’s a California resident or not.
As Rebecca touched on, hard to know how Company C
would make that determination at this point. They
probably don’t have address information. Fertility
tracker apps don’t tend to collect that kind of
information. Can they use IP address? Hard to say.
Hopefully we’ll get more guidance from the California
Attorney General on that.

And, then, are they selling information? Is
this a sale? So are they -- in exchange for the
information, are they getting some valuable
consideration? And assuming that it is a sale of
personal information, is Carla’s deleting the app, is
that an opt-out? Is that them directing the business
to not sell her information? Under CCPA, they say
you’ve got to have at least two methods, a phone
number and a method through the website. So I would
say unless Company C said in its privacy policy, if you delete the app, well, that functions as an opt-out, that probably isn’t a sufficient opt-out under CCPA

Let’s see. Lastly, we’ve got her deletion request. So a year later, she asks the company to delete all information about her. If she’s a Californian, she can’t ask for all information to be deleted. It’s personal information only. So if there is, you know, some kind of an anonymization option, that’s something Company C could take advantage of. Similarly, under GDPR, you’d want -- Company C would want to look also to their privacy policy. Sometimes companies, even if they’re not legally required to, do make promises in their privacy policies about when they’ll delete data. And, then, you’d want to consider whether there are exceptions. So both GDPR and CCPA set out fairly broad exceptions for deletion, so I’d want to consider whether any of those apply.

MS. ARIAS: Thank you. That’s actually excellent issue spotting. You’ve covered actually a lot of my follow-up questions, which means you did a great job.

But let me -- let me open it up to the rest
of the panel. I would love to know if you guys see any other issues that Tracy didn’t cover. And let me actually make that question a little bit different and kind of maybe bring a little bit of the last panel in, where Professor Fred Cate said, you know, we should be focusing on the harms. I’m curious if you all see any harms or any privacy implications in this hypo, that maybe are not covered by any of the laws that Tracy covered.

Jay, would you like to take a crack at that?

MR. EDELSON: Yeah, sure. Yeah, I actually wanted to respond to a lot of what Professor Cate said, so you kind of opened the door. First of all, I think the idea of de-identification is kind of a myth, and so when companies start talking about that, I get skeptical. Years and years ago, before Silicon Valley got really good at figuring out what we do and who we are, Netflix put out a contest to see if people could come up with a better algorithm for picking movies. And they put out -- things seemed totally innocuous. Just no names and just here are some movies.

And news reporters were able to actually tie that to specific people. And the level that the really smart companies are able to do that with is shocking. If you have almost any three points of data...
-- geolocation, for example, but anything even broader than that -- you can find out who somebody is. What’s really scary to me is that they’re selling this information to pharmaceutical companies who could do whoever we -- you know, whatever we want with it, whatever they want with it.

But I want to go back to Professor Cate’s kind of preliminary point, which is that we shouldn’t worry about consent. And I think he didn’t have a chance to fully expound upon this, but it makes some intuitive sense. As consumers, who really reads all these privacy policies? So what does it matter if these companies say, by the way, we’re actually going to be tracking all of this stuff and then providing it down the line to somebody else? And the answer is not because the consumers read it, but because others read it.

So for example, when Snapchat for a day decided that they weren’t going to permanently delete all the snaps, nobody read that in their privacy policy except the blogger, and then it became big news, and Snapchat said, oh, we can’t do this anymore. So I think that’s the real reason why consent is so important and why companies have to follow that.

MS. ARIAS: Lothar?
MR. DETERMANN: Just one point. I would say that the pharma companies, of course, developing new cures that would benefit Carla and many other people -- but I’m probably just an optimist on that. And I wanted to add to Tracy’s excellent list of issue spotting that we have the California Medical -- Confidentiality of Medical Information Act on top of the list that she provided that covers with HIPAA-like rules also providers of hardware, software, and online services since 2015 and requires opt-in consent for certain authorizations.

They have to be handwritten -- that’s real fun when you have a mobile app. And they have to be signed in a typeface no smaller than 14-point type, although it doesn’t specify the font type, only the size of the font. Clearly separate from any other language presented on the same page, executed by a signature that serves no other purpose than to execute the authorization, signed and dated.

Plus, we have a separate law that requires consent for the collection of medical information with direct marketing purpose. That’s Civil Code 1798.91, I’m cheating here, reading from my own book, making the point that we already have hundreds of laws, and I think we didn’t need the California Consumer Privacy
Act on top of all of these, unless we repeal some of them or preempt them on a federal level.

MS. ARIAS: Yeah, Al.

MR. RAUL: So, first, just responding to Jay on the de-identification, you know, if we can’t rely on de-identification, we’re really cooked in terms of innovation, picking up on what Lothar said. I mean, these public health advocates want this data for a reason, the pharmaceutical companies as well. You know, progress, innovation will stop, and artificial intelligence will be completely developed elsewhere.

So if a statute says, like CCPA, that -- and, by the way, HIPAA -- says that you can work with de-identified data, we should strive for that. And, of course, de-identified data, if it’s been anonymized, isn’t even personal information under the GDPR. We could talk for weeks and months and years about pseudonymized data, but I know there are, like, two minutes left, so we won’t.

A couple of other issues to note. So Carla wants Company C to delete the information about her. It’s not clear from the hypo whether the information that remains with Company C is in de-identified format, but if it were, under the CCPA, the company would not have the obligation to re-identify Carla.
from that in order to find it and delete it.

And, then, the request is coming in a year later, so a year later is about 12 months. So the look-back provisions are 12 months for what a company needs to go back. So, you know, maybe depending on when she asks and what remains, you know, the company may not be able to find it, re-identify it, and delete it 12 months later.

MR. EDELSON: Can I follow up?

MS. ARIAS: Yes, please, Jay.

MR. EDELSON: Alan, I’m just curious, in terms of stifling innovation, so let’s say you’re that company, you come to me and I’m a lawyer, and I say you can do this, you just need to add a sentence saying, by the way, we’re going to collect this information and we’re going to send it on and we’re going to try to make it anonymous and here’s how, and that’s what we’re going to do. You think companies are going to say, oh, it’s not worth that?

MR. RAUL: Oh, you mean in other words if you make disclosure of the de-identification plan in advance?

MR. EDELSON: That’s all that’s required for most privacy.

MR. RAUL: Yeah, no, I think that’s right,
but I think also we can assume it. When data is collected that it is possible -- I mean, it’s contemplated under HIPAA, under CCPA, under GDPR, you know, I’m sure under other regimes as well, that it can and will be de-identified. And, you know, under HIPAA, to be sure, it’s perhaps more regulated if the party who is de-identifying it doesn’t have full data rights to it.

But it’s sort of a standard, right? De-identified data is tantamount to anonymized data, really, and people deal with anonymized data all the time. So I don’t think it would be hugely burdensome to just say that. You know, we can de-identify your data and then use it for other socially beneficial purposes or commercial purposes, which is, you know, analogous to socially beneficial. Or we could just assume it, that that’s what people are going to do with data, that if they can figure out a way effectively to de-identify it within the consistency of the relevant statutory regime, then they’re free to work with it because it’s to everybody’s benefit.

MS. ARIAS: So I have a question from the audience, kind of following up on the discussion between Jay and Alan. So given that there’s -- my understanding from the audience -- is that the
definition in California of the resident is somewhat wide, and, obviously, we have the 12-month look-back period. So the question from the audience is, does the wide resident look-back period essentially create a national right. What are your thoughts on that?

MS. SHAPIRO: So in the sense that because you can’t -- it’s so hard to identify who is a California resident that you will effectively have to give these rights to all Californians. I know of companies that are considering that implementation, that they’re looking at what data they have about users and there are some that determine that they don’t have sufficient information -- with the guidance that we’ve gotten so far from the AG’s office. Hopefully, there will be something more when we get the regs, but that they might have to just apply this nationwide.

MS. ARIAS: Okay.

Yes, please, Rebecca.

MS. ENGRAV: Two thoughts on, in essence, the de-identification piece. To me, if we think de-identification actually works, you know, if we believe in it, if we decide whatever the standard is -- maybe it’s the kind of circular piece way that’s defined within the CCPA; maybe it’s the existing FTC standard.
Maybe we come to something better. But if we believe in that, then there’s really no point in, Jay, to your point, notice and consent to people because, like, what are they noticing and what are they consenting to if we believe that, in fact, there’s no reasonable chance that they’ll be identified? If we don’t believe in it, if we think, well, we can do the best we can, but, actually, a really good college student could figure out who you are from this, then I think we need to, all of us, including recipients, including cities and governments that say they’re receiving data in de-identified fashion, need to stop telling consumers and kind of over-promising what de-identification means.

So I think, like, you can’t answer the question, should consumers have a right to either consent and opt-in or opt-out from some sort of de-identified third-party sharing without also coming to a conclusion about what de-identified means, and if we actually think that it still exists as a concept.

One other piece to your point --

MR. EDELSON: May I just say, I agree with you 100 percent. First time.

MS. ENGRAV: That’s unusual.

MR. EDELSON: Yeah.
MS. ENGRAV: There is a way in which even a truly de-identified sharing -- so now let’s posit a world in which it’s really, really good. Could still, in fact, create some form of personal psychosocial harm to someone. Jay and I probably don’t agree on whether that’s actionable under a law, but what if the public health advocates or the pharmaceutical companies are also receiving other information about these folks? What if they are receiving the race, the age, the ethnicity, the income status of these users? And what if they are using that as part of how they’re formulating whatever their treatment plans or modalities could be?

You know, this history is a pretty bad -- our country has a bad history in some sectors of making public health decisions about people from different races. And maybe there’s a person who uses this app and wants the benefits for themselves but just doesn’t want their data to go into that data set, even if it’s never going to be associated with them. So that just could be a different -- a way in which even de-identified data sharing could present a risk.

MS. JILLSON: These are all great issues that you’ve all raised, but in the interest of time, we’re going to move on to the next hypo. So here we
have Company D, which sells smart coffee makers that
can be connected to an alarm clock app. The company
installs a microphone but does not disclose its
presence. Three years later Company D announces a
software update that will activate the speaker so that
it can respond to commands to make coffee. The
company will also data-mine the voice recordings to
improve the product.

Calvin Consumer is concerned that Company D
may have recorded his conversations. He wants to
access all data about him.

Jay, what are the privacy implications about
this scenario, and what can Calvin Consumer and his
friends do about it?

MR. EDELSON: I think they can do a lot.

But, first, I just love this hypothetical because it
gets to the heart of the debate about privacy. I
always think about my mom when I -- when I evaluate a
privacy case. And I ask, would she care about it?

And when you look at the hypo, just on its face, her
answer would be no. What do I care? I’m probably not
going to use the voice-recognition software. If it’s
in there, there’s no harm to me. Jay, you should
become a dentist. Why are you wasting your time with
this?
Here, though, and this was touched on by a previous panel -- this is why it matters so much. So the first thing I would look at as a plaintiff’s attorney is I would actually look at biometrics law. Illinois, for example, the Biometric Information Privacy Protection Act, which has become very active over the last couple of years, talks about voiceprints. And what we’re seeing is more and more companies -- Google and Amazon, for example, are very good about this -- where they’re using people’s voices and identifying people by their voices. So you actually help train their systems. They know when I’m talking to Alexa as opposed to my neighbor.

The issue with that -- and this was touched on by the last panel -- is that once you’re able to connect someone to their voice and you’re able to track how they speak, you can find out a ton about them. The example given on the last panel was Parkinson’s disease, which seems somewhat intuitive. There are some other examples which are less intuitive.

One is research has been able to figure out whether someone is depressed, just by listening to recorded versions of their voice over time. Another thing is there’s an Israeli company that claims to be
able to come up with personality profiles about people just based on their voice. So they can predict insurance claims, risk of loan defaults, likelihood of employees leaving their jobs.

This is all the type of stuff which could result because someone got a coffee maker and wanted to be able to say, you know, I want some coffee. So again, I would look at the biometrics law, Illinois specifically, and I would say, did you get proper consent? Beyond that -- and I know I sound like a broken record -- it always goes back to just general consumer protection statutes.

We have a very similar case, and I want to mention to almost all the hypotheticals we have some similar case here. But one that’s very similar, we’re suing Bose, you know, the high-end headphones. And we allege that they were capturing some information and not telling people. And we sued them under consumer fraud statutes and also wiretap claims. The court accepted the consumer fraud claims, and when it came to damages, something which I would bet some of these people would be skeptical about, they accepted our argument, which is that people are overpaying for a product if they don’t understand that that product is secretly spying on them.
So when we bring these cases, we bring experts in who do surveys and say, okay, how much would you pay for this nice set of Bose headphones? And someone says -- whatever. I don’t know what the price is. I get cheap headphones. But $400, $800, whatever it is. Then they say, okay, now they’re secretly recording the songs that you’re listening to, and how much would you pay for that? And the answer is significantly less. And so those are the types of theories that we would be focused on and that are really starting to pick up steam.

MS. JILLSON: Would anyone else like to respond to anything that Jay raised or anything in this hypothetical?

MS. SHAPIRO: I would also be thinking about -- it wasn’t clear to me from the hypo, are they getting a consent for the software update? Is it an automatic software update that gets pushed out, such that you don’t know that the microphone is suddenly recording you? Is there a "wake" word so that it’s only recording me when I indicate that it should be recording me, or is it just going to always be on and always recording? And if that’s the case, then I would be thinking about ECPA and state wiretap law concerns for recording conversations.
MR. DETERMANN: I would just highlight that Jay’s mom wouldn’t have paid less for this coffee machine because she didn’t care, and I think that makes the point on some of this harm argument or speculation here.

The other point I would make is that the Computer Fraud Abuse Act already prohibits accessing other people’s machines without consent to collect information. That’s an old federal law that we already have. And we do have, for example in California, eavesdropping statutes that would capture, if wiretapping doesn’t apply. So I think we already have, again to make this point, myriad laws that probably already cover this. And I think the California Consumer Privacy Act was not necessary for this one.

MR. EDELSON: Since my mom was invoked, she would -- she would care because if you said you’re tracking -- it depends what the implications are. If they’re not doing anything with it at all, and they’re not storing this information, they’re not doing what these Israeli companies are doing or other companies and they’re trying to figure out who my mom is and what her social well-being is like, then she probably doesn’t care, and there’s probably not a very good
claim out there for that.

But if they’re doing all those nasty things, her view would be -- and I know this, because she’s my mom -- her view would be I don’t want to buy this for any cost. And that’s really what we’re seeing, that if the companies are misusing the data and not telling people what they’re doing with it, most people, they don’t say, well, I’ll still buy it but for $20 less. Most people say, you know what, I’ll buy different headphones or I’ll buy a different coffee maker.

MR. RAUL: Is Company D going to, in addition to activating the microphone for voice activation of making coffee, is it going to impose an additional charge on Calvin because all of a sudden, the device has more features? And is it going to impose that charge, you know, surreptitiously without, you know, getting opt-in?

And, also, is it going to start a subscription service that will also, you know, poll Calvin -- or Jay’s mom -- would you like me to order coffee for you, and then all kinds of other, you know, commercial applications like that? You know, clearly, this is something that shouldn’t be done surreptitiously, but if an additional feature is activated by the company, again, one could look at
that as progress or getting something for free, if
it’s disclosed, obviously. But it isn’t necessarily
all that different from improvements in firmware, or
software, that, you know, are just mediated through
code rather than having a, you know, a physical
speaker and microphone in the device that people
didn’t know.

So would you not want -- you know, again,
firmware and software updates that resulted in the
possibility being eavesdropped on, yes, that should
clearly be disclosed as well. But you could really
look on the bright side and say, wow, you know, my
product has just improved for free.

MS. JILLSON: So let’s assume here that the
software update that will activate the speakers also
brings with it security updates, bug fixes, since
updates are often bundled. So if the only way to
forgo activation of the speaker is to ignore that
whole update and miss out on these bug fixes and
security updates, is that problematic?

MR. EDELSON: Yes. I agree.

MS. JILLSON: And does current law
adequately address that situation?

And, Alan, you had a very affirmative or
strong reaction to that. So how --
MR. RAUL: Yeah, no, I mean, it does --
that seems -- you know, I don’t think -- I’ll put
myself in your shoes. I don’t think the Federal Trade
Commission would have a tough time thinking, oh, maybe
there’s something unfair, deceptive about that. Maybe
it was -- you know, and this was a take-it-or-leave-it
proposition where there’s -- you know, there’s an
intrusion here, the possibility -- again, there may be
other controls on it, that the hypothetical may not
fully address in terms of security controls so that
there’s no chance that there’s going to be an
inadvertent activation of this without the consumer’s
knowledge.

But, you know, if the idea here is to put
the consumer in a position to possibly being exposed
to being unintentional to the consumer recorded, you
know, then burying it with other security updates, you
know, that would seem unfair, and if it’s disclosed
inconspicuously, potentially deceptive.

MS. SHAPIRO: I think the FTC could arguably
bring an -- that would be a place where you could
actually bring an unfairness case and have a tangible
privacy injury, which would be, I paid $50 for this
coffee maker; I was not told it was going to record
me; now it records me. I’m assuming that it’s not --
there’s no “wake” word, there’s no opt-in, there’s no way to turn it off, and I’m now out $50. Like, that would be a tangible harm.

MS. ENGRAV: I think it probably depends, though, exactly what the security risks are that we’re talking about that you will not be getting the patch for. I mean, it sounds from the hypo that if you don’t install this update the only thing that’s really smart about your coffee maker is that it can connect to your alarm clock app. You know, even if that were hacked kind of -- I mean, you know, I don’t know, maybe.

But it just seems like we need to think through, because if you’re not getting that update and you’re choosing not to activate the speaker aspect to it, perhaps the risk to you of any -- you know, there’s no actual real risk. Like, what’s going to happen from --

MS. SHAPIRO: Although is the consumer ever in a position to make that judgment?

MS. ENGRAV: Right.

MS. SHAPIRO: Right? Like, how bad is this big bug?

MS. ENGRAV: Well, if we’re looking at it under unfairness, then the consumer doesn’t have to
make that decision. I mean, unfairness isn’t about
notice or consent anyway. I’m just thinking it might
not actually be an unfair situation.

MS. SHAPIRO: But does the consumer really
have a choice? If they’re being told this is a patch
to update a bug and they don’t know if this bug is
catastrophic, they’re going to have to install it.
And now they’ve got a machine that’s recording it
where they didn’t consent to it.

MS. JILLSON: And should we be taking into
account third-party externalities? So if the bug
would affect, you know -- gets hacked, it becomes part
a botnet, there are external harms.

MS. ENGRAV: The botnet of coffee makers?
MS. JILLSON: Stranger things have happened
in IOT, but in the interest of time, we can move on.

MS. ARIS: Yeah, so let’s move on to the
last hypo of the day. Company E offers a free
internet browser to consumers. It mines browsing
history and behavior to infer demographic information
about consumers, which it sells to advertisers. It
turns out that one popular data set is for females 10
to 12 years old. Candace Consumer, not Jay’s mom,
requests access to all data Company E stores about her
so that she can correct any inaccurate data.
Alan, last but not least, you want to walk us through the privacy implications?

MR. RAUL: Thanks, Andy, and, you know, I don’t know that it’s really fair to have had a hypothetical about coffee, you know, at 4:45 in the afternoon, you know, just as everybody is starting to doze off to hear me address this hypothetical.

But, you know, today is a very exciting day, I think, in our field, and I’m going to explain. Maybe it was already talked about. But, you know, normally, as some of you know, you know, I talk about -- because you’ve asked us, Elise, and you, Andy, asked us to speak as everyone else has about the way different platforms might approach these hypotheticals. So, you know, normally, that would involve a recitation of the US leadership on privacy going back to 1791 and the Bill of Rights and the right to be let alone in 1890 and the FTC Act in 1914 and the Privacy Act, which embodied the fair information practice principles in 1974, Gramm-Leach-Bliley in 1999.

But today -- yesterday, in the UK -- and I don’t know if anybody else has addressed this -- but there was a -- the UK Government announced an online harms white paper that is going to lead, according to
the UK, to new regulation with strict new enforcement. And I really commend this to everyone’s attention. And it may turn out to be relevant to this hypothetical, which is about 10 to 12-years-old kids. And that is it’s about online harms. And I know that Professor Cate addressed this, Lothar did earlier, and there has been a lot of discussion about harms.

When one goes to privacy discussions, frequently we’re talking about regulations and procedural and administrative hurdles and not so much the bad things that can happen as a result of privacy infringements. Well, the UK in this white paper yesterday, it’s 102 pages long. It has charts and a litany of real harms.

Now, it does purport to not cover privacy and data protection, which is the mandate of the Information Commissioner’s Office, or hacking, but the fact is, it really addresses everything that we’re worried about online for concerns about children -- exploitation, sexual abuse, addiction to the internet, access to inappropriate content -- real harms.

And so I really do say that this is a development, I think, that we should all be thinking about in future regulation. We know that in the NTIA request for comments that the Commerce Department
issued, it also focused on harms. So I think that as we consider these hypotheticals and, you know, especially this one, which is about, you know, dangers online to children, so the first -- turning not to the broad focus on the right approach, philosophical approach to privacy regulation, so question -- this, obviously, since it’s 10 to 12 years old, it raises the question of whether COPPA would apply.

And so the first question is does it really cover -- does COPPA apply here? This is an internet browser. So COPPA applies to operators of websites and online services. Clearly, is a browser in this context such a website operator or online service? You know, ISPs are not considered, as the FTC has stated, to be covered. Are browsers? Is it analogous to, perhaps, a plug-in or an ad network in this context? You know, so I think that’s an issue.

Just some other basic questions. Does the browser have to provide a privacy policy under COPPA? If it applies a privacy policy under CalOPPA, if it’s collecting information about California residents? So is this browser in some way directed to children? You know, even though the popular data set concerns females 10 to 12 years old, there’s no indication as to whether they -- they know that the children are --
you know, that the people that they’re tracking are 10 to 12 years old, or that the service is in any way directed to 12 years old.

Is there a persistent identifier involved that would be a potential trigger under the Federal Trade Commission’s regulation, under COPPA, or what is the basis for tracking so that it would invoke COPPA? Passive tracking, if that’s what’s going on, would be certainly within the scope of COPPA, and as well, the CCPA. And, then, questions of access rights, how do you -- in a prior version of the hypothetical, we didn’t say who the -- whether it was Candace Consumer’s relationship -- and I guess it’s not here, either -- whether this is -- what is the relationship of Candace to anyone in the data set of 10 to 12 years old?

Is the company going to be able to find data or to -- under CCPA they wouldn’t be obligated to re-identify data. Under COPPA, is the data -- if it is attributed to a persistent identifier, is this something that is pseudonymized or de-identified. Is re-identification going to be possible? And is it going to be required? Is there a right to rectification of the data, to correction of inaccurate data?
Under COPPA, there’s access by the parent to the data about the children if they can be verified, but not necessarily to correct inaccurate data. Under the GDPR, there might be such a right under CCPA, likely not a correction right, although, certainly, an access and a deletion right.

Thinking about other parties’ obligations here, is there an obligation of the advertisers who are receiving this data? Do they have knowledge? I mean, are there websites where they’re -- this is analogous to a plug-in perhaps, where the website has invited this browser in and is somehow responsible for the information that the browser is collecting on behalf of the websites?

And, then, are there obligations on the part of the browser company to provide other COPPA requirements for protecting the security, confidentiality, integrity of the personal information of children, if it’s -- you know, if it’s not de-identified? So we have some age issues here under COPPA. This data set for females 10 to 12 would be covered as under 13. Under the GDPR, the consent age is -- consenting to processing as specified in the GDPR is 16, but member states in the EU can lower that to as low as 13.
Under the CCPA, we have two standards for age, as everyone has heard a lot about: under 13 for opt-in by the parent or legal guardian; under 16 for affirmative consent to sell data from the child itself. The tracking and profiling would raise heightened concerns, heightened requirements under COPPA and GDPR. I’ve talked about the persistent identifier and is this really capable of identifying Candace or anyone else in the data set?

Under -- you know, under COPPA, would COPPA apply at all -- again, because with regard to the deletion right, COPPA applies to data that’s received from the children. The CCPA also applies to the deletion right, applies to data that is received from the subject, not anything about the subject. There’s some ambiguity in that, although the statutory text certainly suggests that deletion of data received from children is the way the CCPA works. The GDPR, on the other hand, concerns any data about any individual.

So the authentication issues here will be significant. How does Candace Consumer or her parent verify that they have a right to correct this data or access this data? And I think those are the issues that I would flag.

MS. ARIS: Great, thank you. And those are
great.
So I’m going to open it up on the panel, and I’ll give you a choice. You can either react to the hypo, or since we are nearing the very end of our panel, you can either give your closing thoughts maybe on some of the current laws and the applicability and maybe some of the gaps in the current laws as they stand as they relate to privacy.
Lothar, do you want to start?
MR. DETERMANN: I’ll do the reaction to the panel, and Alan made a great analysis already. I’d observe this: The California Consumer Privacy Act would require parental consent or opt-in consent from 16-year-olds, and that will lead like COPPA has already that people are excluded from websites. I think that’s the main repercussion of this. Children are excluded. Every website policy says you have to be 13. In the future, it will be 16. And that is the main achievement here.
None of our hypotheticals actually delivered any harm to us. Did you notice this? We have here that demographic data is sold but not what could happen to the children? We heard that on other panels, that is there, and I don’t want to diminish it. But I would say we have to act against those

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555
harms. If somebody is exploiting the children, let’s do something about exploitation of children but not necessarily about collecting information about them.

If in the fourth hypothetical, the coffee machine could be turned on and create voiceprints and they’re being abused for something, let’s prohibit that but not necessarily prevent coffee machines from reacting to voice commands instead of pressing a button.

And I could go to the other ones. The pharmaceutical development, the public health -- none of these delivered harm, and, yet, the CCPA, the GDPR pretty much prohibit everything that is being done. And I think that is symptomatic to many of our hypotheticals and something we should all think about as we’re exploring new approaches to privacy.

MS. ARIAS: Jay, any thoughts?

MR. EDELSON: Yeah, and I’m glad for that lead-in because I wanted to talk about harm, too. I think this is the great philosophical debate about privacy, which is do we adopt the model where we have to wait until something really, really bad happens, and then someone can sue or do something about it?

And, I mean, it’s an awful example, but the idea of child exploitation, that we know that a
dangerous situation is being created, but we’ve got to wait, and then when that happens, that child can somehow bring suit and recover damages as if that’s going to be terribly helpful.

The best analogy for this is in the data breach context. And I think the FTC has really taken a lead, where they have brought data security lawsuits, where they’ve seen that companies have vulnerabilities, and they recognize that there may be a hacking that could happen, and once there’s a data breach, the idea that you can make people whole is just not true. It disrupts people’s lives. There’s identity theft and all of that. It’s just not worth it to them to go to court and try to get some amount of money back. What they really want is to avoid the data breach in the first place.

And so the FTC, as leaders in this, have started bringing -- or for actually many years -- have brought suit and have said, you know, when you have vulnerabilities out there -- and often they’ve matched it to what the public-facing statements are -- so we protect your privacy, and have fallen short on that, they go in and say that’s consumer fraud and you got to fix those vulnerabilities.

And I think that’s really where privacy laws
should be focused on, how do we prevent the really bad harms before they happen as opposed to just wait for it and then try to fix it.

MS. ENGRAV: I’ll just respond to one of those points a little bit. I think that taking the data breach example and the FTC bringing enforcement actions, what that hasn’t solved for, though, is there are undoubtedly other companies out there right now with the exact same vulnerabilities, and they aren’t sophisticated enough to even know they’ve been hacked.

So if what we want to do is decrease the risk of that even happening, we’re going to have to find a way to move beyond case-by-case enforcement after there’s a big issue, because right now, it’s not a level playing field. The companies that are investing huge amounts of money in data security and doing a really great job of it, maybe because they’ve already had an enforcement action, maybe just because of their size.

The other, you know, companies, you know, all those great mom-and-pops, all the wonderful small startups that we hope develop and bring the wonders of the digital economy to all the small communities in America, they’re not doing any of those things. So if we think that there are data security steps that are
fundamental to even doing an online business, we have
to find a way to communicate them in actionable ways
and not just rely on case-by-case enforcement.

MR. RAUL: I agree with Jay. We shouldn’t
wait until it’s too late to protect consumers and
citizens from harms, but I think it’s incumbent upon
policymakers and the interested public to try to
identify those harms, act only insofar as -- or
balance, you know, do a cost-benefit analysis to
protect the public against those harms, but not
stifle, you know, innovation and economic opportunity
and so on.

And if we aren’t smart enough to think in
advance about the harms we want to protect the public
from, we’ve got the backstop of Section 5 of the FTC
Act and the state UDAP statutes, you know, to
prosecute unfair and deceptive acts and practices.

What I -- you know, I commended the
audience’s attention to the UK online harms white
paper, which really chronicles so many different harms
that are really -- you know, online manipulation,
disinformation, you know, exploitation, and attacks on
children -- that it’s a great place to start.

Another place to go to as well is the Spokeo
decision in the Supreme Court, where the Court, while
not finding standing in that case, that is to say concrete injury for an alleged violation, the Fair Credit Reporting Act, the Court did say that intangible injury can be real and can be actionable, but it’s got to be grounded in some recognized either statutory principle where Congress or another legislature has identified a harm, or in the common law or in the long tradition that we have of protecting people against highly offensive invasions of privacy.

So I think we -- you know, we can look to those models, and this is also in the request for comments of the NTIA -- to come up with a new framework. And you can also look, by the way, if you read all of the GDPR, as I did recently in order to address the question of what does the GDPR say about harms, and the answer is that most generally, it speaks about just abstract infringements of fundamental rights and freedoms. And these are important fundamental rights and freedoms, but was there anything concrete in there? And it’s data security -- Jay’s point -- you know, data security, which I think we can all agree that’s important.

And then it gives concrete examples of where potentially profiling, and the FTC wrote a great
report on, you know, big data inclusion or exclusion, but where profiling could lead to actual, tangible impacts of being denied credit, being denied insurance, being denied employment, being denied other opportunities. So, you know, even the GDPR and the EU knows how to frame real harms, and, of course, which is what the US tried to be in Gramm-Leach-Bliley for financial harms, HIPAA for healthcare harms, Electronic Communications Privacy Act for electronic harms, video privacy, you know, educational privacy, et cetera.
CLOSING REMARKS

MR. TRILLING: I apologize for being in the position of cutting off our discussion. On behalf of the Federal Trade Commission, I just want to take a few seconds to thank all of our panelists and speakers for sharing their insights and providing us with an outstanding discussion today. I also want to thank our audience and our online audience.

We look forward to another interesting day tomorrow when we’ll be discussing the role of notice and choice, the role of access, deletion, and correction. Then we’ll have remarks from Commissioner Rebecca Kelly Slaughter. And after lunch, we’ll conclude the hearing with a panel on accountability, and a two-part panel discussion on the adequacy of the FTC’s toolkit for protecting consumers’ privacy.

With that, we will resume the hearing tomorrow at 9:00 in the morning.

(Applause.)

(At 5:07 p.m., the hearing was adjourned.)
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