FEDERAL TRADE COMMISSION

DATA TO GO:
AN FTC WORKSHOP ON DATA PORTABILITY

TUESDAY, SEPTEMBER 22, 2020

8:30 A.M.

VIRTUAL EVENT

FEDERAL TRADE COMMISSION

I N D E X

P R O C E E D I N G S

- - - - -

WELCOME AND OPENING REMARKS

MS. SIGNS: Good morning and welcome to Data To Go, the FTC's workshop on data portability. My name is Kelly Signs. I'm a Deputy Assistant Director with the Bureau of Competition at the FTC. On behalf of the entire FTC workshop team, we're delighted that you're joining us today via our live webcast.

Before we begin our program, I have a few administrative details to cover. First, a video recording and transcript of these proceedings will be available on our workshop webpage shortly after the event. Our intent is to a create a lasting resource for anyone who's interested in this important topic.

Second, as with any virtual event, we may experience technical issues. If these occur, we ask for your patience as we work to address them as quickly as we can. We will let you know if there are going to be any significant delays.

Third, we'll be accepting audience questions via our dedicated email address, dataportability@ftc.gov. Due to time constraints, we may not be able to get to all the questions, but we will review all the ones that we receive.

Finally, please join us on Twitter. Our Twitter handle is @FTC, and we'll be tweeting using the hashtag #datatogoftc.

And now I have the great pleasure to introduce our first speaker, Andrew Smith. Andrew is the director of the FTC's Bureau of Consumer Protection. He came to the FTC from the law firm of Covington & Burling, where he chaired the financial services practice group. Earlier in his career, Andrew was a staff attorney at the FTC where he led the agency's rulemaking efforts under the Fair Credit Report Act.

Andrew has written extensively on consumer protection and financial services issues, and served as Chair of the American Bar Association's Consumer Financial Services Committee. Welcome, Andrew.

MR. SMITH: Thank you, Kelly, and welcome, everyone, to Data To Go, an FTC workshop on data portability. Thank you all for tuning in. I'm sorry we can't all be in the same room this morning to interact with one another in person, but I'm grateful that we still have the ability to host a workshop on such an important issue with experts from around the world. This is the FTC's third virtual workshop, and I'm confident that it will be another success.

In the last few years, data portability has emerged as a hot topic in both antitrust and consumer protection circles. Freeing up data promises to increase consumers' choice and control their own privacy. It could also foster competition by, among other things, lowering barriers to entry. But there are risks. While there may be privacy benefits to allowing consumers greater choice and control, increased data flows raise serious questions about how to make sure that data is kept safe. This convergence of issues has presented the FTC, which has both competition and consumer protection missions, with the opportunity for staff from across the agency to collaborate.

This workshop is a prime example. And I'd like to thank Jarad Brown and Kate White from the Bureau of Consumer Protection; Andrea Zach, Kelly Signs, Chris Grengs and Ryan Quillian from the Bureau of Competition; Ben Smith from the Bureau of Economics, and Guilherme Roschke from the Office of International Affairs for bringing us this event.

The term "data portability" can mean different things to different people. For some, data portability refers to the ability of consumers to receive a copy of the data about them either for their

own conveniences or to move the data to another service. For others, data portability means the transfer of data about multiple individuals so that, for example, a business can easily move its customers database from one vendor to another.

Across the globe and here in the U.S., we have seen various approaches to portability. Some approaches such as in the EU and California have focused on an individual's rights to portability. These jurisdictions have enacted general consumer privacy laws, and although there are differences in their regulations, both jurisdictions give consumers the right to receive their data in a format that more easily allows the transfer of that data to another entity.

India, on the other hand, does not have a general privacy law, and its data portability initiatives aim to increase consumer access to services, especially health and financial services.

Other approaches such as the UK's Open Banking initiative and the interoperability rule at HHS Office of the National Coordinator for Health Information Technology, have taken a sector-specific approach. They have each created secure standardized methods for data to be transferred with the goal of

providing consumers with better access and control over data and increasing competition.

At the same time as these government initiatives, there are industry-wide efforts such as the Data Transfer Project that are working on ways to create open source service-to-service data portability platforms to allow consumers to easily move their data between companies.

We're fortunate today to be joined by regulators and other experts and stakeholders to discuss their experiences with these rules and projects. We'll start the day with a presentation from Peter Swire, who will provide relevant background on the issue and set the table for the rest of the day's discussion.

Then our first panel will offer a look at data portability initiatives in the EU, India and California. Our second panel will explore sectoral approaches to data portability. Our afternoon sessions will take a more general look at data portability, and beginning with our third panel, which will discuss the attributes, benefits and challenges of data portability initiatives with an eye toward the twin aims of protecting consumers and promoting competition. Our final panel of the day will tackle

some key concerns confronting data portability initiatives -- security, privacy, standardization and interoperability -- and will consider some solutions.

So I'm looking forward to hearing all of our panelists' thoughts on these issues. The goal of today's discussion isn't a broad policy pronounced measure or legislative recommendation. Rather we intend for today's program to be a contribution to the broader discussion among global policymakers about how data portability can empower consumers and promote competition without compromising data security.

For example, the OECD has recently sponsored similar events on data portability, and we also will be paying close attention to other developments such as the CFPB's recently announced effort to make rules under the Dodd-Frank Act to facilitate consumers' access to financial data.

Before I close, I want to thank the panelists for giving us their time. Because this is a virtual event, many of our speakers are participating from other time zones. So a special thanks to those of you who are joining us for a very early morning or a very late night. And thank you to everyone who is attending virtually. We appreciate the opportunity to engage with the public on this important issue, and I

hope you enjoy the FTC's Data To Go. We will open with a presentation from Professor Peter Swire that will begin at 8:40. Thank you.

AN OVERVIEW OF DATA PORTABILITY: CONCEPTS AND TERMINOLOGY

MR. SWIRE: Hi, everybody. This is Peter Swire. I'm calling -- speaking to you from my cluttered office in Atlanta, Georgia, where I'm a professor at Georgia Tech. My thanks to the FTC for organizing this fantastic workshop today.

Could we have the background slide, please? So as an overview of what I'm going to do in about 15 or 20 minutes, I'll give a brief story of my own background, including a 125-page study on data portability that's available this week. I'll explain three reasons for the current interest in data portability, then talk about some terminology that I propose as a way to make it clear that portability could be transfers of one person or of many persons, as Andrew Smith just said.

I'll try to talk about the dilemma here that antitrust and other factors tend to open data flows, but privacy and security tend to close data flows. And the proposed answer to the dilemma is to have what I call a portability and other required transfers impact assessment, a PORT-IA, which is a structured way to try to figure out how to work your way through these different issues.

In the course of talking about the PORT-IA, I'll talk about results from sectoral case studies that I've done in the United States and Europe, and I'll explain the importance of having a multidisciplinary assessment of these issues. Next slide.

So, as I said, I'm a professor now at Georgia Tech. I'm wearing my Georgia Tech colors on my tie today. I'm also a senior counselor with the law firm of Alston & Bird. I've worked on privacy and related issues since the mid-1990s. In the late 2000s, I worked in the White House in the U.S. Office of Management & Budget as the chief counselor for privacy with U.S. government-wide responsibility for privacy policy. That's when HIPAA and Gramm-Leach-Bliley happened, for instance.

If you get certified as a U.S. privacy professional, I'm the lead author on the textbook for taking that test. And I've been a professor at law schools and elsewhere in privacy, in cybersecurity, and in antitrust law. So I have a relatively unusual background of having taught all of these subjects.

I've also worked at the intersection of privacy and antitrust for quite some time. In 2007, the FTC asked me to testify about that intersection,

and I proposed that we could understand privacy as a nonprice or a quality aspect of competition. And this approach of a nonprice aspect of competition has been widely adopted since then.

In 2013, after the draft of GDPR was released, with a co-author, Yianni Lagos, I wrote an extensive article on data portability, and I decided over a year ago to come back to data portability to see if we could try to make sense out of what to do next. Next slide.

So, again, as Andrew said, there's a number of reasons for the current interest and for having this workshop today. One thing is that we have new broadly applicable laws on the right to data portability. The GDPR in Europe went into effect in 2018, just two years ago. In California, the California Consumer Privacy Act went into effect in 2020, at the beginning of this year. And so for very large numbers of companies, they’re facing an obligation to have an individual right of data portability.

A second reason for these debates are the intense policy debates that everyone on this call probably knows about, about the digital platforms. What about privacy? What about antitrust and

competition issues? And these intense debates are happening both in the European Union and the United States. And in my research project, I try to give roughly equal attention to both the EU and U.S. I've worked on EU law for many years.

A third reason for the current interest is there's multiple sectors, important sectors, in the United States and Europe that now have mandated data flows. So, for instance, HHS, the U.S. Department of Health and Human Services, issued it's healthcare interoperability rule in final form in February of this year, March, I guess. And in EU, the open banking in the UK and the Payment Services Directive for the entire European Union, is in the late stages of being implemented. So you have healthcare, you have financial services, major sectors that are subject to these data portability issues. Next slide, please.

So for the terminology, because it's been confusing to talk about the different kinds of data flows, I suggest one -- others may find better ways to define it. And so for me the right to data portability is about an individual right to transfer data. And especially if you talk to European Union lawyers, but I think also California lawyers,

portability with a small “p” is becoming a term of art. If a European lawyer says there’s a portability issue, that means there’s an issue of one person having their data transferred to a different place. And so that’s an individual right to transfer it to that person himself or herself, whereas an individual right to transfer from the original service to a different service, that's an individual transfer right. For me, that's a small “p”.

Now, there’s also a lot of discussion, again, as Andrew Smith mentioned, about having mandates, proposed or actual now, to transfer entire databases, to transfer data involving more than one person. In Europe, this has typically been called data sharing. So you’d move a lot of data from this database to that database, and they call it data sharing.

In my view, that’s a vague term because data is shared in so many ways for so many different reasons around our digital economy. And so my paper proposes calling these “other required transfers.” It’s either portability about one person or it’s other required transfers about a lot of people.

And so to give an example of other required transfers, in the United States under the new rule

that HHS issued this year, a hospital or doctor's office has a right to transfer all of its records from one software provider to another one. That's a massive transfer of records partly so it doesn't get locked into the particular software provider or cloud provider it has today.

And that kind of law is very familiar in the European Union. They have a regulation on it to go to the General Data Protection Regulation on personal data. They have what's called the free flow of data regulation for nonpersonal data, for other business data, and it has these same kinds of rules of transfer of one database from one place to another. Next slide, please.

So continuing on terminology, the word interoperability features very highly in discussions of these kinds of issues. And I suggest that the proposed definition of interoperability has to do with the technical ability of two or more systems to exchange information. That might be common data formats, you know, having a picture look like a picture. It could be common communication protocols, how my computer speaks to your computers to structure the interactions between the computers. And it can include other technical mechanisms that enable

operation of two or more systems. So, for me, I think it's least confusing, most clear, if we use interoperability to be a technical word about transfers from one place to another.

Now, the HHS rule, which they call the interoperability rule, I think can learn from the discussions that this workshop is having today, because HHS has used the word "interoperability" in what I think are three pretty different situations.

So it applies to the technical issues I just described higher in this slide. Second, it applies to individual portability. So under HHS you'd be able as an individual to move your data from a provider to your app on your phone. And it also applies to other required transfers such as moving a doctor's office's records from one cloud provider to another.

So for me the first of these threes would be interoperability; the second would be lowercase "p" portability, and the third would be other required transfers such as to a new cloud provider. Next slide, please.

Now, one reason certainly for having the interest we have here and having the regulators we have from different countries in the world, is that this individual right to data portability has gained

great new prominence in recent years. So under Article 20 of the GDPR, data subjects -- individuals -- have a right to receive data or transfer it to a third party in most cases that they have provided to the controller. So if I use a service, I have a right to transfer it to myself or to others. And the language in the GDPR has been picked up in a lot of laws around the world. The transfer has to be what? It has to be without hindrance, super quick, easy, without hindrance portability. That's the law in the European Union.

California picked up similar kinds of words. So in the California law that's on the books and in effect today, there's an individual right to access data, but that access has to be done in a way that is portable -- there's our word "portable" -- and a readily usable format. So the service must provide the consumer with the data in a portable and readily providable format.

So conclusion on this slide, just since 2018 -- and now it's 2020 -- we've had implementation done in the European Union and in California -- and California is economically significant. It's often said that California would be the fifth biggest economy in the world if it was a standalone economy in

terms of gross national product. Next slide, please.

So that brings us to our dilemma. Overall, as we think about this, should we open up or close down data flows? And for antitrust and competition reasons, there are many compelling reasons to open data flows. Let's just imagine that there's important databases in our economy, valuable databases about people that are large, that contain a lot of people's data. Well, that's what we live with. We have those in the major services and lots of other places in our data-oriented economy.

So the idea for antitrust people is if more companies have access to that commercially valuable data, then those companies can compete, they can innovate, they can have a more effective competition around that valuable resource. Okay. That's what the antitrust people's intuition is.

For people who start from privacy and cybersecurity, often they're looking to have ways to close data flows. What if data goes to the wrong person? Well, that's not good. The game for privacy in cybersecurity is to stop it from getting to the wrong people. So cybersecurity tends to focus on unauthorized access. That's a hacker getting into the data, pretending to be you to transfer the data, or

that's an insider who's not supposed to look at the data getting it. That's the cybersecurity angle.

The privacy angle is more about what focus we have on access that should be authorized. And often in privacy, those complicated set of rules, often the rules are let's be cautious unless the individual consented or basically knew what was going to happen.

So in terms of antitrust, we've seen clear evidence that the interest in portability from regulators in Europe and the United States. The Federal Trade Commission Director of Competition, who I believe is speaking later today, in February said the breadth of additional relief that may be considered include obligations to provide data. And you can see the rest of the quote on the slide. Well, obligations to provide data sounds like data portability. And we have the workshop today showing the FTC's interest in this issue.

In Europe, their Commissioner for Competition, Ms. Vestager, discussed the prominent position of data in digital markets, which I think we all accept, and she said the need to ensure the possibility of entry, new entry, by more competitors may argue in favor of mandating access to data. And

those other required transfers, those mandates, are central to what we're talking about. And the European Union released it's European data strategy earlier this year with many discussions of portability. Next slide, please.

So to respond to that dilemma, I'm suggesting in my study that's available today at ssrn.com to create a well-designed Portability and Other Required Transfers Impact Assessment. And the method here is similar to privacy impact assessments that are required for U.S agencies, for instance, in the United States where the data protection impact assessments that are required under GDPR.

And the methodology for the study, for all this work I've been doing for over a year, has been first to try to draft structured questions of what the impact assessment would ask, to try to have a systematic assessment, and then test those assessments against all those case studies that I showed you earlier. And then the case -- the structured questions change quite a bit. We learn from all these case studies. And we can validate the structured questions based on these numerous case studies across different geography, across different sectors, across different types of data. Next slide, please.

So to look at the case studies a little bit more, for the EU and the U.S. we looked at phone number portability. You can go to one phone company provider and keep your phone number when it goes to another provider. That's been on the book for almost 20 years.

Now, this portability approach has been super successful. But after I've looked at it, compared to other case studies, it looked like a misleadingly -- a misleadingly easy case. Most people want their phone numbers known to the other people in their lives. So it's not a privacy problem. They want the data out there. So you don't have that tension between privacy and competition that we see in some other sectors.

The study looks at a U.S. financial services and EU financial services case study, and the Dodd-Frank Act of 2010 where there's rules that are supposed to be developed now by a U.S. agency requires portability for consumer financial records.

Looking at EU and U.S. healthcare -- and in March this year we've been talking about this HHS rule where individuals get portability to their smart phone apps, that's small P portability, and there's other required transfers to move to a new healthcare

provider.

I also have a case study on open data for government databases. You can think of when government has open data requirements, it's a mandatory portability out to the internet. People can get the data. And there's a set of laws in Arizona and three other states that were recently passed that have to do with when auto dealers are locked into a provider for their software services, what are the rules for being able to move to a different software provider? Next slide, please.

So now we'll do a very quick overview of the top-level questions in the PORT-IA, not the sub-questions. First, the first question is, define the challenge or opportunity that leads to a possible port. Where does the data come from? Where does it go? What types of data are covered? What specifically are the legal requirements? You get your engineers in here to do a data map and then you look at the legal requirements so you know what you're talking about. You have to do that first. What does the world look like? Next slide, please.

For benefits, here's a set of questions. Question two is, assess the PORT rationales based on competition. And there's subquestions on network

effects, on lock-in effects, on barriers to entry and on other competition issues.

Next, assess innovation and other commercial benefits due to the PORT. If we move the data around, maybe there'll be new and cool companies that can do things with it. Question four is, assess the noncommercial benefits due to the PORT. And this is where individual rights come in. The individual has a right to control their own data. And that's not primarily about finances. It's about some self-determination about your right to data.

Question five is, assess the regulatory benefits that come from this new rule. Question six is, watch out, there might be less benefits, reduced benefits, because maybe there's technical feasibility problems. It's not interoperable. Maybe there's market limitations. People aren't actually asking for the data. So you might dream of a huge benefit and it might be less in practice.

And then question seven is, assess the incentives of those presenting evidence for the benefits. Maybe there's a company that's trying to get data from another company. They have a reason to say portability is wonderful. It doesn't mean they're wrong, but at least you should recognize why it is

that they're doing what they're doing. Next slide, please.

So once you've done these data portability benefits, let's do our risks and our costs that come from portability. Question eight is, assess the privacy risks. And there's subquestions about identify data, de-identify data, data of third persons.

Next is assess the security risks about unauthorized access or problems with security in transit. Next in question 10 is, assess the risk from the PORT that may arise for either security or privacy reasons. And there's two here that I go into more detail in the paper. One of them is the risk of onward transfer. If the data goes to the receiving service and then they send it on to A and B and C after that, is it still under control for privacy and security?

Another one is that people might use standards. Companies might use standards to discriminate so that they get the data and other companies don't get the data. And if they have market power, that might be something that the antitrust people would look at.

Question 11 is, assess the risk to

competition from the portability initiative. If the three biggest companies in an industry get together and set standards so they get all the data and nobody else does, then there's an antitrust risk that comes from them having all the data.

Question 12 is, assess the regulatory and legal consequences. Question 13 is, look at other obstacles to adoption and other costs that maybe haven't been included in the list yet. And the last one is, assess the incentives for those preventing evidence of risks of costs. There might be companies that love having the data. They're going to say portability is very, very dangerous; don't make us move the data, it's just too scary. They may be right, but you should check to see what their incentives are. Next slide, please.

A couple of other points. I talked to the FTC. They asked for a couple of other clarifications or distinctions that help us understand how these PORTs, these portability and other required transfers, might work. And the first distinction is whether you take action as a government before or after the violation. So one approach is to have regulation ahead of time, ex ante regulation.

So if you want to do that for HHS, for

instance, for the healthcare interoperability rules or Dodd-Frank for financial interoperability rules, you don't have to find an antitrust violation first in the healthcare sector. You don't have to find an antitrust violation first in the banking sector. Instead, you say we have enough reasons here to pass a law, to pass a policy and mandate, even though we haven't found an antitrust violation. That's ex ante, that's before the violation regulations.

Another approach is to think of portability as a way to use as a remedy when there is an antitrust problem. This is expost, afterwards. So this has been -- I spoke at the ABA antitrust section a few months ago, and the antitrust lawyers in the U.S. are thinking, oh, we need a remedy. If there's a mess under antitrust laws, require portability and that way we might undo the mess.

And the court might order portability. There might be a negotiated consent decree. And the regulators who are tempted by these kinds of remedies say, well, breaking up the company, that's radical. Maybe just have the data move around a little bit, let's have some portability, that's less radical. So portability seems attractive because it's not as decisive an action. It's a more moderate action.

Okay. So that's the end of this slide on before or after the violation. Next slide, please, on general or sectoral.

So another distinction of the kinds of rules we have about portability is some of them are general portability rules that applies to furniture stores and drug stores and every other thing. And GDPR does that in its right to data portability, and California does that as well. It's across different business sectors.

But we've also seen that there's been a lot of sectoral rules. In the United States, where we're often careful about regulation, we have it for phone numbers and financial services. That's 20 percent of the economy. Healthcare, that's 20 percent of the economy. And we're seeing it pop up in other places like the auto dealer software standards. So there's different kinds of laws that go across sectors or vertical by vertical. Next slide, please. And I've just got two more slides to go.

So now that we've gone through this, there's some reasons to consider using this portability impact assessment. One is we have all these new laws and all these new proposals. So we'd have a regular way to look at all of them informed by what we've learned already.

Another reason to do the impact assessment is that most people haven't taught privacy and cybersecurity in antitrust. They've had a life that's led to lots of other good things. And so in many instances it'll be best to have a team to assess portability proposals. You want your economists and your technical engineers and your lawyers and your privacy people, your cybersecurity people, your antitrust people. If you can find people who can do all those things, then you can work through this checklist.

Another advantage is that the PORT-IA provides a systematic technique to assess so that regulators case after case, or company situation after situation, can be consistent. For antitrust regulators, or courts, they can realize that privacy and cybersecurity not just be offered as a pretext or an excuse. There's real issues here.

For people who work on privacy and cybersecurity, they can realize that consumers benefit from having greater competition. And so the benefit for users on the privacy side and the benefit for users on the competition side both are going to those individual data subjects. So that might be something to think through.

And then the suggestion is the private sector can assess their most promising PORT initiatives, looks like when it's going to work the best or what are the risks if they try to do it. Final slide, please.

So, in conclusion, for opening up data flows, for transferring data, portability of data, there can be great benefits for competition, antitrust, to have innovation, to have freedom of individual choice. These are valuable reasons to consider portability.

We also have strong reasons to consider closing data flows: privacy and cybersecurity. So there's benefits from opening and there's benefits from closing, and so we need, in order to come to some mature view of the situation, to look at both of those.

The Portability Impact Assessment provides a method that's essentially agnostic about each proposal. You don't know -- when you give me a proposal, I don't know whether it's going to have net benefits or not. So then let's work through what are the benefits and costs for this required transfer. Can we increase the benefits? Maybe we can focus transfers on where it really, really helps

competition. Can we reduce the costs? Maybe we can tailor privacy rules so that they're very effective over here, but when there's benefits from transfers we don't have to be as strict.

And so for this complex and increasingly important topic, the PORT-IA can assist policymakers, can assist companies, I hope, stakeholders, people watching today, to reach better decisions on this -- better informed decisions.

I'll be back with you today for Panel 3, but for now I thank the FTC for holding the workshop and having an opportunity to have all these great experts from around the world gather today. Thanks very much.

DATA PORTABILITY INITIATIVES IN THE EUROPEAN UNION, CALIFORNIA, AND INDIA: CASE STUDIES

MR. ROSCHKE: Good morning, everyone, and welcome to this, our first panel of the day of our data portability workshop. My name is Guilherme Roschke. I'm counsel for International Consumer Protection at the FTC's Office of International Affairs.

In this, our first panel today, we hope to set out the baseline and begin to explore three approaches to data portability. Three of our panelists are here to represent each of these approaches, and our other two panelists will also bring their expertise in how they've seen data portability in action.

I'll now introduce our panelists. Inge Graef is Associate Professor of Competition Law at Tilburg University. She's affiliated with the Tilburg Law and Economics Center and the Tilburg Institute for Law, Technology and Society. Inge is an expert in the areas of competition law, platform regulation and the governance of data. She is Co-chair of the Digital Clearinghouse initiative, which aims to facilitate cooperation, dialogue and exchange of insights between regulatory authorities across Europe

and beyond in the areas of competition, data protection and consumer law. Inge is also an appointed member of the European Commission's expert group to the EU Observatory on the Online Platform Economy.

Rahul Matthan is a Partner at Trilegal. He is part of the telecommunications, media and technology, or TMT, practice group of the firm. Rahul has advised on some of the largest TMT transactions in India. He has also been involved in a number of policy initiatives in the TMT space, including assisting the government in preparing the country's privacy law. Rahul is a published author and a regular speaker across the world on matters relating to emerging technology and the law. He also writes Ex Machina, a weekly column on the interface of law and technology.

Karolina Mojzesowicz is the Deputy Head of the unit responsible for data protection at the European Commission, Directorate-General for Justice and Consumers. She was on the European Commission's representatives in the interinstitutional negotiations with Parliament and Council on the General Data Protection Regulation, and is now responsible for its implementation in the EU.

Karolina previously served as a member of the EC's legal service, focusing on EU competition law and international trade law. In that capacity, she represented the EC in numerous cases before the European courts and the World Trade Organization panels and appellate body. Karolina studied law in Poland, the Netherlands and Germany, where she obtained her Ph.D. in 2001.

Stacey Schesser is a Supervising Deputy Attorney General for the Privacy Unit and Consumer Protection Section of the Office of the California Attorney General. Her recent matters include People v. Equifax, People v. Uber, and leading the team charged with drafting regulations for the California Consumer Privacy Act.

Stacey began her career at the Attorney General's Office in 2007 in its Criminal Division and has worked in the Privacy Unit since its inception in 2012. Stacey received her JD from the University of California-Berkeley School of Law, where she wrote on privacy issues for the California Law Review and received a BA from Douglass College, Rutgers University.

Gabriella Zanfir-Fortuna is Senior Counsel for the Future of Privacy Forum, where she leads work

on global privacy developments and European data protection laws. She has a Ph.D. in civil law from 2013, the University of Craiova, with a thesis focusing on the rights of the data subject, including the right to data portability, and an LLM on human rights.

Previously she served as the Legal and Policy Officer for the European Data Protection Supervisor in Brussels, where she was involved in the legislative practice of the General Data Protection Regulation, and the assessment of the EU-U.S. Privacy Shield. Gabriella is coauthor of GDPR, a Commentary, from Oxford University Press of 2020.

So I'll begin by asking each panelist a question for their initial contributions, and we'll move on to a more conversational Q&A later. We're also listening to audience questions via our email address, dataportability@ftc.gov. Finally, you can also follow along on Twitter via #datatogoftc. So let's begin.

Karolina, the GDPR effected a broadly applicable data portability scheme over two years ago. We'll get into the experience a bit later. But for now can you explain the GDPR's data portability requirement, including what circumstances it applies

to who gets the data and what data; is it all of their data? Karolina, over to you.

MS. MOJZESOWICZ: Hello. Thank you. Thank you for having me. Indeed, the GDPR introduced a new right, a right to portability, which is related to but not equal to right of access which existed already previously, so under the previously applicable laws in the European Union.

Why did we want to introduce portability right concerning personal data? Well, in the European Union we made very good experiences with the use of portability. For example, in the area of the liberalization of the telecom markets, so the portability of the telephone number have proven to liberate, to open up, the consumers in order to try new alternatives than telecom operations.

Well, this thought led us to introduce this right in the GDPR, General Data Protection Regulation, in order to further empower the consumer in order to allow for more innovation and in order to also enable consumers to choose services also on the basis of their privacy friendliness.

So what our idea was is that a free consumer who does not have the sunk cost, let me call it, of the data which he/she provided to a certain business

controller, this consumer can take this data and move it freely to somebody else who offers him/her a service which is better from different point of views, point of view of innovation but also point of view of privacy friendliness.

This has the procompetitive effect for new commerce on the market for maybe also SMEs, small and medium size enterprises, and prevents the so-called locked-in consumers which already used for several years platforms, social media, and provided a lot of data.

Now, when does this right apply on the basis of the regulation? This right applies only if the data subject, so the individual, provided this data on the basis of the consent, so consented, the business controller to use this data, or on the basis of contract.

The GDPR, for all those who are maybe not so familiar with the GDPR, allows for several legal bases to process data, so the tools to use data and consent and contract to only some of them. Other legal bases are law-tasked, pursued by public administration, or also legitimate interest.

Well, if the data is processed by somebody on the basis of law or task of a public

administration, or legitimate interest, this data, the data subject of individual does not have the right to port this data. So the data can be ported only again if this data was provided by the data subject on the basis of consent or contract.

So this is when. Now, which kind of data can be ported? Not all of this. Obviously only personal data. And the personal data, so not anonymous data or data which is not concerning the individual who wants to use this right. Which data? Now, data provided, the regulation says very clearly it needs to be data provided to to the controller. But -- so as to the full effect to this right, the European Data Protection Board, which gathers all the European data protection authorities, the enforcers of the GDPR in Europe, specifies that this data provided by means not only data which was actively and knowingly provided by the individual to the controller, but also data which was observed by the controller, so the business, by the virtue of the use of specific service, by this individual service, which is offered by the business.

So what is meant here is the search history, the board in its guidelines provides also that it can be traffic data or even location data. The very

important difference here which needs to be done between this data actively and knowingly provided and data observed on the one hand is the difference between data inferred or derived by the data controller, by the business. And such data is being defined as data created by the data controller on the basis of the data provided by data subject, the data which is inferred or derived, so created by the data controller. Imagine it will be the profile kept or analysis made on the basis of the behavior of data subject while using certain service and the consequences of this observation, this cannot be ported.

So to give you a very clear delineation between which data can and cannot be ported, I would say that “provided by” included which data provided by which can be ported, is data which relates to an individual's activity or observation of individual behavior, but it is not the data which results from the subsequent analysis of such a behavior.

I think it’s a very important difference because it attaches because it has an impact also on the intellectual property of the business who is processing the data.

What are the restraints to the right? So I

cannot port data when my exercise of the right would have an adverse effect on other individuals, on third parties. What is is meant here? If I port -- because it's sometimes difficult to confirm when would it be the case because, of course, for example in my telephone book, in my mail contacts, there are also -- there is also personal data of third parties which will be then affected by my exercise of the portability right.

Well, again, here the delineation line, and as if a "lackmustest," when the -- when my exercise of the right would amount to somebody else being adversely affected, will be when the data which is ported will be processed by this new receiving business, by the new controller, for a purpose which has completely nothing to do with the purpose for which it was processed by the initial data controller.

I think I gave you as even outline of what the data portability is about in our EU understanding and how the GDPR conceived this right. But let me know if I can adhere something.

MR. ROSCHKE: Okay. Thank you for introducing us to the GDPR approach. We'll get to more of that in our discussion later.

Our next question is to Stacey in

California. Stacey, the CCPA includes a requirement that under certain circumstances data be portable. Can you detail the portability requirement in California, including what data it applies to and how it interacts with the right of access in the CCPA?

MS. SCHESSER: Good morning. Thank you so much for having me. It's really an honor to be here joined by such experts in the field on this panel. And thank you to the FTC.

Before I begin, I have to give a typical disclaimer that the views I share here are my own, and the Attorney General may not share these same views.

With that, I'm going to dive right in. The CCPA, the California Consumer Protection Act, contains one small reference to portability, and that is in Section 1798-100(d). I'm just going to read it briefly just so that people are oriented to what the statute provides. "A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, personal information required by this section. Information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent

technically feasible, readily usable format that allows the consumer to transmit information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide information more than twice a month in a 12-month period."

So there's a couple things at play there that I just wanted to walk through here as it relates to that one reference to portability. This is a significant section. It comes at the outset of the law, and it lays out the framework for access rights within the law.

CCPA does not prohibit collection. It only requires that there be notice at or before the point of collection. But as it relates to access rights or what we refer to as the right to know, portability is going to be balanced with verification, costs and timing. Right? So, the idea is that data can be portable if it's verified. It needs to be provided free of charge. And the timing is no more than two times a year to balance the interest of the burden on the business with the rights of the consumer.

What's interesting enough is that these access rates apply to presumably all data that is produced in response to a consumer request both from a

general description of categories down to the granular, specific pieces of information that are collected about the consumer.

The reference that I'm -- the point of the statute that I'm referring to is in 1798.110, where it goes through what the consumer is entitled to receive as part of this disclosure. That includes the categories, the general broad categories of personal information a business has collected about the consumer, the sources from which that -- the categories of sources from which the personal information is collected, the business or commercial purposes for collecting or selling personal information, the categories of third parties with whom the business shares personal information, and then the specific pieces of personal information it has collected about the consumer.

So that is all that's required to be provided in this portable format. So I can't really speak to the motivations for why portability is only mentioned once and how it's structured within the framework of the legislation. What I can infer is that there was this motivation to balance consumer protection, ownership, control of data, all reasons why we see portability as a right in other sectoral

laws within the United States, such as, for example, the medical privacy law, HIPAA, that's been around for a very long time.

What I can speak to is the regulations that take into consideration the impact of the portability of data. So when we were -- the attorney general has authority to draft regulations that operationalize the requirements of CCP for businesses and clarify how consumers can exercise their rights under the law. And so concerns about portability were really at the forefront of our minds when we were drafting the regulations.

One specific area in which portability impacted the rules was in the requirement that businesses not disclose any of the personal data that’s set forth in 1798.81.5. These are data points that more of the classic data points. So, for example, name plus Social Security number, your account information related to your finances. So these information points are particular here because it could place the business in somewhat of a catch-22 where they’re required to provide the information, but it also could be triggering some of their breach obligations if that data goes into the wrong person's hands.

So the regulations state that you cannot disclose those actual data points, but you have to inform the consumer that that's part of what you collect in a general category sense.

The other area in which the regulations really address portability has to do with verification. As many people know, the CCPA did not define what is included in the verifiable consumer request. That was something that the legislature specifically charged the attorney general with figuring out –- so the verification and what principles a business has to consider before disclosing information from both the general categories all the way down to specific pieces, because verification is required for any type of request to know or right to know, is what –- is part of what a business must consider before they go and provide all of this information in a portable, usable format.

So considering the risk of harm and the sensitivity of information is part of what the general principles for verification lay out in our rules. We were considering things like identity theft, but also far worse, what happens when the wrong person has access to data. Complete records of specific pieces

of personal information could fall into the wrong hands, and then you could have something far worse than just, you know, stealing somebody's identity, but even committing great acts of harm.

The one small exception in the regulations has to do with businesses are not required to produce in a portable format certain data that needs specified criteria, including if the data is not searchable or not reasonably -- in a reasonably accessible format, as well if the data is used solely for legal or compliance purposes and not sold.

These regulations were concluded based upon public comment that we received saying that this would be a huge burden on businesses to go and search, for example, a consumer's personal address that was on the return portion of a check. So that is one example in which portability is not required.

From a practical standpoint, you know, we have one data point which is an attorney that works for me who has made a request, and what does that mean when he actually receives all the information? According to him, he said I got one gigabyte of files of gibberish from a large company with a hell of a lot of data about me, some photos, but mostly text or code, and it's not particularly useful for switching

over to another similar platform.

So while there is a robust right to receive your data in a portable format, I think there are lots of practical implications about how that can be consumer-friendly.

MR. ROSCHKE: Well, thank you for sharing your experiences, Stacey, as well as your quite detailed knowledge of the law.

So we'll continue our virtual journey across the globe by turning now to hearing about the developing data portability framework in India.

Rahul, you bring us the perspective of how India is creating data portability infrastructure outside of their privacy law, which is still in development. Can you introduce your role in this and describe the data portability infrastructure being developed in India? What is hoped to be the impact of this developing infrastructure?

MR. MATTHAN: Thank you, Guilherme, and thank you to the FTC for inviting me to be a part of this panel. I was just listening, you know, to the comments of GDPR and CCPA. And as you mentioned, Guilherme, we in India don't have a privacy law -- a full-blown privacy law at this point in time. It's still making its way through Parliament.

But I think, you know, just to set the context of what India has done, India is digitizing at a furious place. So, as you know, we're a large country with 1.3 billion people. 1.2 billion of them have a digital identity at this point in time. And that's what we call the other unique identity.

We also have a tremendous digital payment system. Through COVID and the lockdowns, in the last month alone our Universal Payment Interface, or UPI, did 1.6 billion transactions just in the month of August. And then we've got this -- we're rolling out this huge goods and services tax network which is a very powerful system that essentially is going to keep track of every invoice that every business exchanges between each other as part of commerce.

So two or three years ago, we came to the realization that even though India -- and much of India is still economically poor –- given this rate of digitization, we are going to become data rich far before we become economically rich. And there was this thought to -- you know, to try and figure out how do we leverage this particular situation to try and make it more beneficial to those in the economy who are actually not touched by the financial system.

And, you know, if you think about it, we

have 1.3 billion people. Maybe 300 million of them are on the formal banking system, which leaves a billion people untouched by the banking system.

And so the thought was to try and build a portability infrastructure, a digital portability infrastructure, that will allow people who are not part of the various financial, healthcare and education and other systems to leverage some of the data that is already contained about them in the system to get some benefits. And this is how the idea of DEPA, the Data Empowerment and Protection Architecture, was built. This is essentially a digital framework that allows for data portability from -- and I'll just make up some examples and you can actually apply them in all the sectors. But if you think about the financial sector, if you have -- you know, in order to access -- to get a loan in India, you need to provide evidence of collateral, that is typically some real estate, some property, and a lot of people actually don't have access to that.

But what they do have is a rich history of transactions. And if there is some way in which we can, in a digitally secure manner, present the information of transactions that your bank account has to the potential lender, that may be the basis on

which the lender can give you a loan. And that was the idea behind DEPA.

So what DEPA does is it empowers users to port data from one financial information provider to a financial information user. And in this case, the financial information provider is your bank, the entity that has the data that it needs to provide to the financial information user, which is the lender, that would use this information in order to come to an assessment as to whether it can give you a loan or not.

The core of this is the creation of consent managers. And so what we've done in India is we've, in a sense, disintermediated content from this framework. And so there are consent managers built into the financial system who will manage the consent part of the portability.

And so, you know, once again, just to give you an example, if your lender wants to assess whether you are worthy of a loan, they will send a request through your consent manager to you. And that request, when it comes, says yes, I consent to allow my bank to provide the information that my potential lender wants from me. And once that has been digitally signed, you know, by me saying that I have

consented to provide this information, the information flows on the basis of that digital consent to the lender, and then the lender takes his or her decision on that and provides consent.

You know, there's a lot of detail in this that, you know, maybe we can get to in subsequent questions. But, you know, at the bottom of it, the consent artifact is digital, which means that encoded into the consent artifact is information about the person requesting the consent, information about the purpose for which that consent is being provided, information for -- about how long that consent or that data needs to be kept.

So, for instance, if it's information about a loan, there's no need for the lender to keep that information beyond the time that is required either by its internal processes or even by law to keep that information. And so the digital consent actually has coded within it information about the expiry of the data.

And, you know, so to add another layer, the manner in which consent can be sought is not a carte blanche. So you can’t sort of turn on the spigot, look, I want all the information about the user. There are consent templates which would say that,

look, you can ask for certain sorts of information. One category that's prescribed is all information. And in that manner, once again, we can moderate the purposes for which you can request this portability.

So it's fairly early days for the system. As I said earlier, we don't have a privacy law, but the privacy law that is making its way through Parliament has provisions that would give legal sanctity to the consent manager baked in. So hopefully if it passes in the current form we will have legal statutory basis for this intermediated consent.

But already in the financial system we have seven licenses that have been provided to consent managers they call account aggregators. We already have two working apps for the consent managers. So two account aggregators are already live in the system.

And what's really interesting is that particularly through COVID we've come to the realization that, you know, we need to build out a digital health infrastructure. And there is some very active work going on as part of India's national digital health mission to roll out a similar framework for portability in health. And, you know, that

framework would mean if you need a second opinion you can actually make a request through a consent manager for your digital health information that's stored in some health information provider and port it to a health information user.

Core to all of this, of course, is the standards and the protocols based upon which this infrastructure is built. You know, essentially there isn't much in terms of heavy pipes. This is essentially a protocol-based system where the heavy lifting is actually to get the banks, the hospitals, all of the other participants in this ecosystem to actually change their systems such that they can work with the protocols that create the sharing.

So there's a lot to unpack. I'm going to pause there and let everyone else speak, but happy to get into the weeds in any of this in a little more detail.

MR. ROSCHKE: Thank you, Rahul, for the perspective. And I think we will have time to get into more of the detail.

Our next question is to Professor Graef. Professor, your research has addressed how data portability interacts with other legal interests beyond privacy and data protection. Can you take a

few minutes to introduce some of your research findings in the area of data portability, including its impact on consumers and competition?

MS. GRAEF: Yes, happy to do so. And thank you for the opportunity to speak here. So in these introductory remarks, I would like to focus in particular on what is the impact of data portability, but I will start by making some comments on the nature of concept because I think its nature is really a key factor that determines the impact of data portability. And these are issues that are not only of academic interest to researchers like myself, but I think they also allow us to draw some insights for future policymaking and even enforcement. So I will also try to share some of my own observations on this as well.

So as to the nature of data portability, in my view it is really a hybrid between various interests. So in Europe the concept originated in the GDPR, which is really a data protection instrument which aims to empower individuals to strengthen their control over personal data by allowing them to transfer data and take it with them to another service. So in this sense, data portability really fits with the fundamental rights nature of data protection because it enhances your informational

self-determination.

But at the same time, you can also characterize data portability by the sharing and reuse of data that it facilitates. And here you should keep in mind that the GDPR really serves a dual objective. So it promotes the fundamental rights to data protection on the one hand, but on the other hand it also promotes the free flow of personal data across the EU.

And the second objective, which is more about stimulating the EU's internal market, that objective is very much present in the right to data portability as well. And this is also what brings the concept closer to other policy areas, in particular those of competition and innovation.

And in Europe now you can really see this concept of data portability emerging in many areas, so from data protection to consumer law. It has also already been integrated into competition analysis in some cases, and it also forms part of broader innovation policies, for instance, in the context of the EU's data strategy which was published earlier this year. And you also see it coming up in sector-specific frameworks, for instance, in the banking sector, energy and automotive industries.

So this really makes it a concept with a very hybrid nature. And this hybrid nature also determines in my view what impact data portability can have on consumers and competition. And because of the various interests that's come together in this notion of data portability, there's also still questions about how tensions between these interests should be reconciled in concrete cases.

So one issue that deserves more clarity in my view is what I would refer to as the issue of overlapping legal entitlements over data. And this is an issue that can take different shapes. So we have already heard that personal data can relate to more than one individual. So then the question is how you can guarantee the privacy interests of the other person when you want to port your data.

Another example is that personal data may at the same time be protected by intellectual property rights held by the business, for instance copyrights or trade secrets. And such other legal entitlements can limit the effectiveness of data portability of course, depending on the extent to which they stand in the way of requests of individuals to have their personal data transferred to another provider.

And how exactly these interests and legal

entitlements should be balanced against each other, it's not entirely clear from the text of the GDPR itself. So these are issues that will still need to be addressed through future cases, although some guidance is already available as we heard before. But the application in concrete cases can still raise issues. And until there is more clarity on the concrete application, there is still quite some discretion also from data controllers to strike this balance themselves. And this may not always lead to desirable outcomes because data controllers could point to the existence of some of these overlapping entitlements as a sort of excuse to limit the scope of the data that should be ported.

And the message -- the broader message that I want to give here is that in my view the impact of data portability is not an abstract or aesthetic issue, but it is something that regulators and enforcers can really influence by guiding and steering the implementation. And this is true for how data portability interacts with privacy interests of other individuals, with the IP rights of data controllers, and it also holds, I think, for the impact of data portability on competition.

So then moving on to what the impact of data

portability on competition can be. I think it's still unclear now what effects the GDPR is having in this regard and if indeed the right to data portability is really fostering competition on the market and is really encouraging data-driven innovation, which were things that were expected as a sort of positive side effect because it would be easier with the right to data portability for individuals to switch between services if they could take their data with them.

But at the same time, I also now see concerns being expressed that data portability could actually strengthen the position of established players by letting users invoke the right to data portability to get even more data. And this would then lower competition because smaller firms could then see their users move to the established players with their data.

So one idea to make sure that data portability would really create opportunities for newcomers to innovate could be to introduce what I would call a symmetric regulation and enforcement. And what I mean with a symmetric regulation is that more powerful firms would be subject to stricter conditions. And this could then also include requirements to enable data portability.

And this could be done in several ways. It could happen through antitrust enforcement, for instance, by requiring merging parties to facilitate data portability as a condition to approve a merger, or by qualifying restrictions on data portability as one monopolization or in the EU as an abuse of dominance. And beyond antitrust enforcement in the EU, in fact, the European Commission is currently preparing a proposal for a new legislative instrument, the Digital Services Act, which is also expected to introduce a new ex ante regulation for so-called gatekeeping platforms. And data portability could be one of those ex ante requirements applicable to these platforms.

And, of course, here there are still questions about how to design such requirements, to whom they should apply, but I do believe that his idea of asymmetric regulation makes sense in an effort to increase the opportunities for smaller firms to compete and also to make markets overall more contestable.

And then at the same time, I think still a question is whether data portability is enough to achieve this, especially in markets where there are strong user site network effects where the value of a

service depends on how many others are using it; so, for instance, in a social network. Data portability cannot -- may not really address user log-in because users will still want to be where everyone else is. So even if users would move, for instance, to a new social network provider and take their data with them, they will not be able to reach the friends on the old network anymore. So data portability may not be enough to address the impact of these network effects.

And how data portability can affect competition in markets without network effects, I think will also depend on how actively individuals overall invoke such requests to transfer their personal data. And here I think data portability certainly helps to empower individuals in their individual relationships with the data controller. But in order for competition in the market as a whole to increase, it is not enough that just a few individuals invoke data portability.

So for this reason, beyond data portability under the control of individuals to address risks of market tipping, increasing market concentration data for industries, requirements for businesses to share data with other market players directly may be needed, so without being dependent on a portability request of

an individual, but of course taking into account privacy interests when personal data will be involved.

And I think this may be needed because the porting of data also creates what you can call a positive externality through the better predictions or better search results that all users will receive when an additional user brings her personal data to a new provider. But users typically don't take this benefit for other users into account when they make a request to port data. So for this reason we could expect too little data portability requests to remedy market tipping in data-drive markets.

So to conclude, I think in my view data portability is really a hybrid concept. It emerged as a data protection concept but is now also becoming part of policies aiming to stimulate competition and innovation. And I think to reap the full benefits of the data portability, my observation is that there is really a need to steer its implementation in practice and also to provide guidance on how businesses should handle tensions between interests and those overlapping legal entitlements.

So in my view data portability can certainly empower consumers to make better choices, but also more asymmetric enforcement may be needed to ensure

that data portability will really stimulate competition.

MR. ROSCHKE: Thank you, Professor Graef, for those perspectives.

We'll continue our tour here with a question for Gabriela. Gabriela, can you tell us about the Future of Privacy Forum's work on data portability? We've heard from India, Europe, and California. Can you provide us with a comparative view and what you're seeing and how businesses are implementing these new requirements and how consumers are using them? Is there evidence of this being a burden on businesses?

MS. ZANFIR-FORTUNA: Thank you very much, Guilherme, and hello, everyone. Thank you to the FTC for the invitation to be part of this expert panel and for putting together what seems like an impressive program for today's workshop.

The Future of Privacy Forum is a nonprofit organization that serves as a catalyst for privacy leadership and scholarship. We bring together businesses, consumers, regulators and academics to promote principled data practices by supporting emerging technologies.

We've been following and contributing to the debate on data portability for a long time now both in

the United States and Europe, and increasingly we pay attention to global development.

Well before my regulator experience in Brussels, in my policymaking experience in U.S., I wrote a Ph.D. thesis under EU law on the right of the data subject -- and this is how we call the individual whose data are being processed, the data subject. Data portability was the newest one of those rights, at that time having just been proposed in the GDPR bill back in 2012.

Thanks to that extensive legal research, I know that even if data portability is also seen as a means to facilitate competitiveness on the market and can be deemed more useful in some markets other than others, the European legal system right now recognizes portability of personal data is a right of the data subject. And this means it is a prerogative of the right to the protection of personal data as detailed by the GDPR. Underpinning it is the idea that individuals should have control over how their personal data is collected and used. And it is with this background that I will make my remarks.

In the first part of my intervention, I will draw your attention to three challenges to effective portability that we learned about from our work with

FPF stakeholders. Authentication and verification of their requesters of data -- and we already heard Stacey addressing this a bit -- the social nature of some personal data and the further uses of data by the receiving organization. And then in the second part I will make a couple of comparative remarks following what one of my copanelists had said but also referring to other developments around the world because I think we should pay attention to those as well.

I will start with the lessons learned from practice. And besides the reality that there are very few portability requests from individuals right now, we've seen that one key challenge is the authentication and verification of the identity of the individual making the portability request.

The lack of effective verification and authentication leads to data breaches, so it can pose significant risks. Think of scammers getting all your account data with one click. This is a common challenge with the right to access one's own data, but it has its additional complexities under portability, whose purpose is to make this data much easier to be used for other services, or even to be directly transferred to those new services.

Now, if we talk about interoperability and

allowing third parties to access personal data directly on the platform or from a particular service, this challenge translates into the need to verify, perhaps even vet, the third parties who are given access to data. But who should do that and how can it be done in practice?

Now, a second key challenge is the social nature of some personal data. And by that I mean that often one's personal data also includes personal data of others, like in photos and with conversations. This raises a couple of questions. What kind of permissions, if any, should be required for those personal data of third parties involved in a portability request, or what kind of safeguards should cover this third-party personal data? What happens if the personal data of the third party is ported to a service provider that has weaker privacy protections or weaker security in place? Should anyone have responsibility for requesting or allowing the transmission of personal data to such a service? All these are difficult questions, but they need to be solved if we want to have effective portability that does not lower the level of protection of privacy overall.

Finally, there is the issue of

further uses of the data by the organization receiving important personal data. Does the service receiving personal data as part of a portability request rely on consent? Whose consent, especially when we talk about third-party personal data? Are there any limits on how it can use data?

The receiving party should not be doing surprising things, right, with the personal data they are given access to. The CCPA does not really address risk. The GDPR and other frameworks inspired by it address it through purpose limitation rules and rules on having a lawful basis or processing place for any of the new processing taking place.

But even under those frameworks, there are other issues that appear in practice. For example, there are challenges when those rules intersect with other prescriptive sectoral stages such as the payment services that are taken in Europe, or PSD2, which might have the opposite effect of overly limiting uses of the data being accessed.

In fact, a couple of weeks back we held an expert roundtable, together with our partners from Vrije Universiteit Brussel, to discuss the intersection of the GDPR and PSD2, this payment services directive. One of the key objectives of the

PSD2 directive is to open up the banking sector and encourage participation to the payments industry of nonbanks like emerging PINTEC organizations through data sharing.

Now, we've learned that there are still many unresolved questions when it comes to banks sharing data with third parties. The consumer representatives that participated in the roundtable highlighted that the landscape appears complex to a regular consumer, making it difficult to allow for actual decision making about [indiscernible, brief VTC lapse] to move their data.

One of the biggest challenges identified was the lack of trust among the wider public to move their data across services. A particular challenge highlighted by experts was also the reuse of the data by the receiving service as the result of applying the prescriptive PSD2 rules in the GDPR framework together. For example, it was not clear to them to what extent or on what local ground using data -- with using the data that has been shared for fraud prevention would be allowed.

Another example of our work in this space is the panel which convened at the Computer Privacy and Data Protection conferencing process in January 2019,

where we explored extensive limits and benefits of portability under the GDPR. And we had a chance to get early insight into the data transfer project about which you will learn later on today in one of the following panels.

This is a relevant and interesting industry-led open source effort which shows that data portability can work in practice, but we've also learned about the many challenges those involved in the project had to overcome. And I remember an example that was given within that debate, and it was catalogued as a challenge of a syntactic nature. And the example used was a jaguar. So when a data set refers to a jaguar, is it a car or the animal? And this actually had consequences on whether the data should be ported or not.

Now, I will certainly be tuning in later to hear about the lessons learned on that project over the past three years. As for the comparative remarks that you're referring to, I would say there are two big differences between portability in the GDPR and portability in the CCPA. And we've heard a bit about them.

First under the GDPR, the scope of the right to portability is very nuanced. It's actually limited

compared to the CCPA if we refer to the scope of the personal data being transferred. And we've heard the details about that, and I think the key difference is that the GDPR does not include inferences about individuals within the scope of the right.

Then in the CCPA, portability follows access. It is not a separate right like in the GDPR. As the CCPA -- and we've heard Stacey -- requires all access to personal data to be given in a portable format. So then really portability follows access.

Before I conclude, I would just like to add that for India -- and we've heard from Rahul about the specific project on financial data, but we are also following the personal data protection field that's currently being discussed by the Indian Parliament, which includes a general right to portability and which is actually very broad because it also includes portability of profiles being created about individuals.

Now, in Brazil, the new general law for protection of personal data, the LGPD, which just entered into first last week, also has a broad right to data portability provided therein.

There's an amendment built to Singapore's general data protection law that includes a right to

portability which has some very interesting nuances. It tackles, for example, third-party personal data in an interesting way and limits when such data can be transferred to a third party.

To conclude, there are many difficulties and complicated questions to answer in order to make portability work in practice without lowering the level of protection of privacy and security, including the fact that it doesn't seem to be appealing to consumers or users or the timing.

However, more and more legal systems around the world recognize the ability to move the data seamlessly and securely across services as a part of new generation of rights that individuals have with regard to how their data is collected and used. Thank you.

MR. ROSCHKE: Thank you, Gabriella, for this overview, your initial comments in the comparative perspective and also bringing in perspectives outside of what we've considered so far.

I think now we'll move on to some of our follow-ups. We have a follow-up to Karolina about recently the European Commission issued a two-year report on the implementation of the GDPR, including reviewing the experiment of data portability. Can you

tell us more about what the review showed and what some of the next steps are being considered, including the new European strategy for data?

MS. MOJZESOWICZ: Thank you. Indeed. Well, to some extent what I wanted to say was already covered by the lady who was speaking before me. So, Gabriela, for example, underlined that indeed this right to data portability was not used to its full potential. And we saw that what we have seen that data -- so the individuals do not exercise it so much, they do not use it so much, and that it's so far used within sectors only.

Why? Mainly because of the lack of standardized machine-readable formats and clear indications as to the structure in which the data should be provided so as to port it easily from one controller to another one.

So this is what we have observed. We did not see a lot of complaints from individuals to data protection authorities that they are right -- that they were not able to exercise this right, and mainly probably because they were not using it that much.

But having said that -- and we still think that this potential of data portability needs to be further explored, and this is what we are going to

tackle now with the legislative instruments which we'll be following up, this communication, the paper the Commission published in February this year, and which will be following fairly quickly now, we want to use this potential of data portability also in the context which was so far not contemplated very much, but to push it into the direction of almost as much as possible real-time data portability, and also within different services. So not only from one platform to another platform and so on so as to resolve a competition problem, but so as to exploit if it means to empower the consumer.

And here we are in particular thinking about the possibility to use this real-time portability right in -- the real-time portability in the further development of Internet of Things devices. Yeah, so which we want to resolve by providing standards and more -- and clarifications of the structures in which data should be ported, and by designing appropriate tools by designing this standardized, as I said, formats and interfaces in order to facilitate this exercise so that this consumer put in the center of the future digital economy will be able to switch easily between different service providers, taking different consideration and different aspects into

consideration; also aspect of more privacy-friendly solutions, which we hope will by -- in the case of, let me call it, digital illiterate and privacy-sensitive consumers will start to -- well, work against this network effects which were mentioned before.

And this is what we see, that our consumers start to be in particular now in the coverage times where we moved all to more use of digital services, they start to be much more sensitive about what is going on with their data and are much more proactively looking for services which also bring them this protection which they so far did not receive, so that this will rebalance the network effects probably long-term, because indeed some operators and some service providers, big platforms, have a huge advantage in there.

But, yes, well, I don't want to repeat what was discussed already before. Let me just make one comment. Let's not forget that this portability right, it's exercised on the basis of the General Data Protection Regulation which actually stems from -- it’s there in order to exercise fundamental right. Protection of personal data, it's a fundamental right in Europe.

Therefore, the ideas -- I'm very skeptical as a person only about this idea about degrees of enforcement. It's a fundamental right, and the scope of the exercise of this fundamental right cannot vary dependent in front of whom it's being exercised. And this is also why the GDPR was conceived in, actually, let me call it, size independent, or size not taken into account way, and obligations and the scalability of obligations depends -- goes together not with the size of the enterprise, but with the amount of the sensitivity of data which is being processed, and the possibility of affecting the rights of individuals while this data is being processed.

So this responsibility of the businesses controllers, their accountability goes hand-in-hand with what they do and not how much they do of it, so that we can have enterprises which will be processing enormous amounts of data but of a very nonintrusive nature. And we can have a much smaller enterprise, I would think here about, you know, laboratories working on DNA, the strictest data protection obligations would apply. So this is a little bit of comment to what one of the previous speakers mentioned.

But to sum up, this is a right with a lot of possibility. We are developing on it and you will see

soon the results. And we think that not only it's not being exercised sufficiently, but it's not being -- so often enough, but the areas in which it can be exercised should be expanded, and in particular in this almost immediate way so one can port in the moment when one uploads. Thank you.

MR. ROSCHKE: Well, thank you for telling us about, you know, some of these next plans and also with some of the implications of the derivation of portability from a fundamental rights perspective.

You know, we only have a few minutes left in our panel, but I did want to continue to discuss and see what some of the next steps are, or potential next steps are in our jurisdictions that we're looking at.

Maybe we could take two or three minutes each to hear from California and India about what potential changes are coming up. Maybe we'll go to California first.

Stacey, can you give us some explanations of any potential changes coming in your legislative scheme?

MS. SCHESSER: Sure. I'll try to go as quickly as possible. The one thing I also wanted to note that we didn't touch on is that CCPA contemplates that agents can make requests, including access

requests on behalf of consumers. And so agents is somewhat defined by regulation. There's a requirement that there's reasonable security when data is being transferred to the agent and to the consumer from the agent, as well as a level of permission that needs to be authorized by either electronic or written signature.

And so that, I think, will also impact portability because people may take advantage of agents that can make requests on their behalf. That may include, for example, products or services to make those types of requests and be able to facilitate that.

So with respect to next steps, I think that one of the most important things is that we are enforcing CCPA. We started enforcing CCPA on day one. We have to issue a notice and cure letter for companies regarding alleged noncompliance of CCPA. We are now also enforcing the regulations as they are effective as law since August 14th, 2020. And so a violation of the regulations constitutes a violation of CCPA.

And what we're doing is we're looking at, you know, a variety of different sources to determine where consumers are running into roadblocks for

purposes of exercising their rights, as well as how companies are interpreting what their business obligations and compliance requirements are. So we review consumer complaints, we conduct our own investigations, we even look on Twitter to see what people are talking about, as well as engaging in a good deal of consumer education so that consumers understand their rights.

There may be additional rulemaking on our horizon that could impact this area. And then, of course, there's a ballot initiative in November which does impact how the access rights are going to be for consumers. It's not yet law; we'll know in November what the results of that are.

Interestingly enough, the section I referred to earlier has been somewhat moved around. There's no express reference to portability in the ballot initiative, but it is implied in terms of the fact that, you know, personal information still has to be provided in a format that's easily understandable and technically feasible, machine-readable format. So there's an implication of portability, although it's not as express as in the initial -- as in the original CCPA that's in effect now.

In addition to that, you know, we continue

to amend data protection laws with last year's amendment to the reasonable security law to include biometric information and government issued IDs. And so, again, that requires additional protections when produced in response to a request to know.

MR. ROSCHKE: Thank you for those perspectives.

Rahul, maybe two or three minutes on the next steps in India?

MR. MATTHAN: Sure. And, look, next steps in India, very simple. We want to get this draft privacy law through Parliament. It's currently before the Joint Parliamentary Committee. And even, you know, through this COVID time and with all the lockdowns, the Parliamentary Committee has been meeting, and so we're hoping that when things get sort of back to normal slightly we're going to have the law, after it's been looked at by the Joint Parliamentary Committee, amended perhaps, presented before Parliament and then enacted into law.

And at the same time, a lot of the infrastructure that I described is being built out and a lot of work that's going on there. I think, you know, just listening to everyone, as I thought that it's probably important to put the Indian portability

framework in a slightly different context. We talk about portability, we think about portability, we think about, you know, changing from one service provider to the other.

Being in the portability framework is not thinking about it from that perspective. We're looking to keep our service provider but move that information to another entity where it might be a different sort of use to us. And we do this real-time. We do this with all of -- because it's digital, we've got all of these protocols, particularly in terms of purpose limitations in terms of use and all of those things.

So, yeah, this is slightly different from what Europe and California are talking about, and it needs to go to a shift of perspective to understand what India is doing.

MR. ROSCHKE: Okay. Thank you for that perspective. I think we have time for one more short follow-up.

Professor Graef, what can we say about the distinction between a general approach and a sectoral approach to implementing data portability? We've heard examples of both. Are there advantages or disadvantages to each? And, please, two minutes.

MS. GRAEF: Yeah. So indeed we see general regimes occurring like the GDPR where the right of data portability applies across the entire economy, and at the same time there's also sector-specific frameworks being developed. So the Payment Services Directive 2, for instance, was already mentioned.

So I think to some extent sector-specific regulations has advantages because you can design much more concrete requirements, for instance, in terms of the infrastructure to be used or establishing common standards for portability or what other modalities should apply. But in a way this can also create spillovers to regimes of general application like the GDPR. So if you have various sectors regulated in terms of portability, this could also make the general portability in regimes like the GDPR more effective, because the infrastructure is already there, standards are being developed that may also be relevant in sectors that are not regulated yet.

Disadvantage of purely sector-specific regulation could be that it is not enough in the dynamic context where you also want market and services to be connected, so in the context of internet of things, for instance. So at some point you also want the sector-specific forms of portability

being connected with one another.

And I think one other issue to keep in mind is that it is logical to start from a more sector-specific approach even for implementing more general regimes like the GDPR, but you also need to take into account effects that go beyond the sector as such.

And then one more comment to reply to Karolina's points on the idea that I put forward for asymmetric regulation, so I should clarify that indeed I was not suggesting that the GDPR or data portability only applies to powerful players. It's indeed a fundamental right and it applies generally across the economy. But I think that data portability, because it is a hybrid concept, there is also room for other regimes like antitrust rules or new regulatory regimes that the Commission is looking at in the Digital Services Act to top up additional requirements for firms that have more market power, for instance.

MR. ROSCHKE: Well, thank you, Professor Graef.

You know, I think we've reached the end of our time here. I want to thank all of our panelists for this fantastic discussion. And I know several of you have joined from inconvenient time zones throughout the world, so thank you for that as well.

We've touched on topics such as competition, sectoral approaches, different motivations, different advantages and disadvantages of data portability, which we can continue talking about that for the rest of the day. And, in fact, that's what the workshop will do for the rest of the day.

So this ends our panel here. Please join us for Panel 2 on financial and health portability regimes starting at 10:30 a.m. Eastern time. Thank you.

FINANCIAL AND HEALTH PORTABILITY REGIMES: CASE STUDIES

MS. WHITE: Good morning. Welcome to the second panel of our workshop. We'll be taking a look at some sector-specific approaches today to portability. I'm Kate White, I'm an attorney in the FTC's Division of Privacy and Identity Protection. I'm grateful to be joined today by an esteemed panel with experience in data portability in the health and financial sectors.

In the interest of time, I'll try to keep my introductions a little brief, but I encourage everyone to take a look at our event page to learn more about their expertise and really impressive work.

First, we're joined by Dr. Don Rucker, the national coordinator for health information technology at the the U.S. Department of Health and Human Services, where he leads the formulation of the federal health IT strategy and coordinates federal health IT policies, standards, programs, and investments.

Dr. Rucker has three decades of clinical and informatic experience. He started his informatics career at Datamedic Corporation, where he co-developed the world's first Microsoft Windows-based electronic medical record. He then spent over a decade serving

as chief medical officer at Siemens Healthcare USA. Dr. Rucker has also practiced emergency medicine for a variety of organizations.

Next we have Dan Horbatt, the chief technology officer at Particle Health. Dan's also a life-long technologist who's worked on building global scale big data systems across a number of industries.

We're joined today by Bill Roberts, the head of Open Banking for the Competition and Markets Authority of the United Kingdom, where he led the design of the CMA’s open banking remedies and is responsible for its implementation. He's also a member of the Advisory Group on Open Finance and the Smart Data Working Group.

And, finally, we're joined by Professor Michael Barr, the Joan and Sanford Weill Dean of Public Policy, Frank Murphy Collegiate Professor of Public Policy, and Roy F. and Jean Humphrey Proffitt Professor of Law at the University of Michigan.

Professor Barr served from 2009 to 2010 as the U.S. Department of Treasury's Assistant Secretary for Financial Institutions, and was a key architect of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.

As with the last panel, I'm going to start

by asking each of the panelists to sort of introduce themselves and tell us a bit about their experience with data portability, and then we'll move to more conversational Q&A later. We'll try to save some time at the end for questions. So if you have a question you'd like to send, we are monitoring our email box, dataportability@ftc.gov.

And so I'd like to get started by asking Dr. Rucker, ONC recently finalized its interoperability and anti-blocking rules. Can you give us a little bit of background on their developments and their requirements?

DR. RUCKER: Sure, Kate, thank you very much. And I'd like to say I'm speaking here on behalf of Kathryn Marchesini, who just went out on maternity leave a couple days early for folks who looked at the schedule.

Yeah, so portability of data in health has been, you know, a desire for a long time. If you go back to the -- what is seen as the defining privacy law in the United States back into the mid-'90s, HIPAA, it actually -- you know, the P is for portability. The problem is the A is for accountability. Neither of those actually happened, as everyone knows.

And, so, what has actually happened is much more limited and is sort of fueled by an interesting combination of technology and policy. So I think the first substrate was, if we talk about data portability, what's really implicit in there is that it's electronic data portability as opposed to getting, let's say, a copy of your medical record in a photocopy or something along those lines.

So the first part really was the work over the last 20 years to have electronic medical records be widespread so there was actually data to share. Prior ONC rulemaking, now about probably eight, nine years ago -- eight years ago -- took a stab at portability, and it was really sort of portability in a sort of a very light way because that's what was available.

And that portability was the requirement that providers, so doctors and hospitals, in their electronic medical record products which ONC certifies, that they have a web portal, which was used by a number of patients. Roughly 20 percent of the population has used those web portals to get their information out.

When you look at the web portals, obviously it's -- there are some features to sort of view,

download and transmit the data, but what you get is something that is, you know, a rather complicated file format that one would really need to have a fair amount of tech skills and ambition to move forward.

So Congress, looking at all of that in 2016, passed as part of the 21st Century Cures Act –- so if you remember back to December of 2016, we'd just had a national election, and there was sort of a brief moment where, you know, there was some bipartisan ability or interest to do things. And so most of the Cures Act deals actually with data requirements for the FDA. But there is an entire title in there on interoperability and portability.

And what did Congress want there? When you look at that, the two key things from a data portability point of view was Congress said, first, the data shall not be subject to information blocking, and, second, there shall be standard application programming interfaces, right? And that makes total sense. So if you think about what would it take to get your data on your smartphone, right, into a form factor that's actionable for the public, I mean, that sort of pretty much these days means a smartphone.

In that -- to get that data in there, you have to be able to get the data both legally and

technically. The legal issues, the so-called information blocking, is just unfortunately a reflection that in the U.S., because we don't have a market economy, we don't have a rational allocation of healthcare through market-set prices, it's all done by third parties where we've commingled equity issues but have lost efficiency in a massively harmful-to-the-economy type of way.

In our system, what we have between the 1942 rules on making health insurance a pre-tax benefit and then Hill Burton cross-subsidization ‘46, and the administrative prices in ‘65, the Medicare Act, we really have -- that soup has ended up with a lot of oligopoly delivery systems whose main economic incentive has actually become so large that they’re price set is to payers as opposed to being really interested in sharing the data the way that somebody who's in a consumer competitive marketplace would have had to.

So Congress said, no, that is now illegal as of the law, and also said there shall be application programming interfaces with -- as Congress put it, “without special effort.” What did that all mean for data portability? Well, ONC has just released a couple of months ago our Cures Act interoperability

rule. And we were required to have some allowable exceptions, information blocking for things like security and privacy. There's some complicated things in that on having reasonable returns on investment to the various activities of building application programming interfaces. You know, the challenge is the Congressional intent to have an API can be blocked by just setting the price to be infinitely high. So without having some mechanism to have accountability on prices, you don't have interoperability either. And, of course, most of this healthcare is ultimately paid for by taxpayers, so there was a huge public interest in all of this.

So the information blocking rules are now out there to provide the legal basis to get the data. The other part of it is, are there technical standards? So rather than each vendor being in a position to have their own private APIs to release this data, they can still have their own APIs, and most of them do for a wide variety of business purposes.

We have in our rulemaking required read -- at the moment read-only APIs so the data can come out. There's a two- to three-year timetable that involves data standards. It involves moving to a technology

called RESTful APIs, R-E-S-T, which is the way the modern internet web economy tools work, and then the FHIR standards in healthcare to move that data, so standardized data tools that the app economy can use, and we believe that that will actually result in, over time, in a wide variety of apps and a true ability for patients to have economic control of their health; to take their data and to move it somewhere else if they're not happy.

So we think that is a major, major advance in data portability in healthcare. It's playing out over the next couple of years, so stay tuned. So, Kate, let me turn it back to you.

MS. WHITE: Thanks for that.

Dan, I know you're familiar with these rules. Could you tell us a little bit about your company, Particle Health, and how these rules are affecting, you know, your industry and consumers?

MR. HORBATT: Absolutely. Thank you, Kate. So I just want to start off and say that Mr. Rucker is a hard act to follow. He has touched on a lot of the points that I was going to bring up, so I appreciate the intro there. But this is very much a personal mission for myself.

In 2017, I had a chronic medical condition,

and unfortunately I was hospitalized when I stopped responding to the medication and treatment I was on. As part of that hospitalization, I was unable to collect medical records from a previous specialist team to give them to my current specialist team in a timely enough fashion, and I had to go through a bunch of unpleasant testing to confirm everything that I already knew, but I didn't have the papers or electronic documents to actually prove to anyone.

So as part of that, I realized that this was a mission that I could get behind and a change I wanted to see in the world, and so I helped co-found Particle Health in early 2018 with my co-founder, Troy Bannister.

And, so, the mission that we're looking to accomplish here is we want to build out a very patient-centric process to enable the distribution and sharing of electronic medical records. As Mr. Rucker mentioned, the P in HIPAA is for portability, not for privacy, and you have a number of rights under HIPAA.

You have the right to access your medical records. You have a right to share them with authorized third parties. You have the right to make corrections. You have the right to revoke the consent of sharing at any point. But it's one of those things

where it’s very hard to actually exercise those rights, and the harder it is to exercise the rights, the less likely you are to really have those rights.

And so that’s what we're looking to spin up. We’re looking to act as the stewards of consent on behalf of patients and, using that consent being able to collect their medical records, no matter where they may be, and provide them to either the patient themselves or to authorized third-party companies that they interface with.

So, for instance, if they're looking to onboard into a telemedicine application, they’re looking to participate in a direct consumer pharmacy, if they’re engaging with a care coordination platform, we want to be able to bring the patient's rich medical history with them such that they get treated faster and more reliably than what they might currently have.

And, yeah, so just to reiterate a lot of what was said already, it's great that we're addressing this from both the policy and the technology landscape, from the policy side of things, the anti-information blocking. We already know that it's possible to share these electronic medical records right now for purposes of use, including treatment, payment and operations, as carved out by

the HIPAA privacy rule. But beyond that, like, we're looking at making sure that we're able to collect electronic medical records with patient consent as well, so making sure that patients who would typically have to fax a form or provide a somewhat blank filled out HIPAA authorization form can now do so in electronic fashion, making it easier for them, making sure they know how to actually follow up, see who has their consent, making sure that they know how to revoke that consent at a certain point in the future if they no longer have a business relationship with whomever, and as well from the technology standpoint.

So TEFCA standardizing on the Fast Healthcare Interoperability Resource, FHIR, making it very easy for app makers, for companies, vendors, IT providers to use very robust open-source libraries to work with this data and transfer it and utilize it in a number of ways, all resulting in better patient outcomes. So exciting times ahead.

MS. WHITE: Definitely.

So, Bill, now that we've talked a little bit about the U.S. healthcare experience with data portability, I'd like to shift gears and talk about the financial sector a bit.

Can you tell us a bit about the UK's open

banking rules and why they were created and how they work?

MR. ROBERTS: Okay. Well, let me start by defining what we mean by open banking or what some people these days are calling consumer-directed banking, I think. So by open banking, we're referring to an ecosystem in which consumer or small businesses can, first of all, instruct a bank to share their transaction data securely with a third party, and, B, instruct a third party to move money around in and out of that bank account. So open banking allows consumers to take control of their own bank data.

I just had a further qualification here, which is that we include in the definition of open banking the requirement that APIs rather than screen scraping is used to access that data. It's a much more secure process for both the customers and its provider alike.

So, second, why do we adopt it? Well, the CMA carried out a market investigation which reported in 2016, and that had taken two years, and it found pretty much the same as every other investigation into banking had found over the previous 20 years, which was that the market was dominated by four big banks who between them had over 80 percent of the market.

People didn't switch banks even though they were dissatisfied with their services, with service quality. Banks charged a lot for overdrafts, short-term credit, and the sector wasn't really characterized by innovation at all. New entry and expansion is rare, as small businesses got a particularly raw deal and had limited choices about where they could find money.

So to tackle those problems, we adopted a package of measures, but the center of which was open banking. That was supposed to breathe fresh rivalry into the whole sector to get existing banks to compete more vigorously with each other and, in particular, to allow the entry and expansion of new firms -- fintechs basically -- who would not be banks but would offer banking services. That was the objection -- the objective at the time.

Now, at that time, by coincidence, we were implementing the EU's snappily titled Second Payment Services Directive, PSD2, and that kind of required some of the same things. It required data sharing between payment services, but it didn't specify the use of common standards for APIs. And that was the big difference with what we did in the UK.

What we said in the UK was we agreed

absolutely that APIs should be used to share data, not screen scraping, but if each bank could design and implement its own API, then life would be very difficult certainly for small developers. Bad enough trying to produce a mobile application for three or four mobile platforms. But if each bank -- and there are hundreds of banks in Europe. If each bank had its own APIs, then you would have to make versions for all of them or you'd have to rely on intermediary services to connect you. That's exactly what's happened in continental Europe now, whereas it hasn't happened in the UK.

So we required the -- not all of the banks, we didn't have the powers to do that, but we did have the powers to require the nine largest banks in the UK to agree -- agree to common and open standards for APIs, data formats and security. And though we'd never done anything like this before, and because we weren't in a position at the end of the inquiry to specify exactly what those standards should be, we had to figure out some way of evolving them with the industry but in such a way that the stakeholders' interests were met, too.

So we did something that we hadn't done before, which was that we required -- because the CMA

has awesome legal powers, and we used them to require the banks to make their best endeavors to reach an agreement over these standards. But because no matter how awesome your powers are, you can't compel the two people to agree with each other because they can always blame the other person for the lack of consensus, we created what we called an implementation trustee, and this person would act as the chair of the group which would discuss these issues, but he or she would have the power at the end of the day to say, well, I heard what everybody said, there's no agreement here, so I'm going to decide this for you. And we had never done that before. I think it was quite unusual amongst regulators to impose or delegate, almost, rules to a third party.

Can you still hear me?

MS. WHITE: Yes, we can hear you.

MR. ROBERTS: Can -- you can hear me? Okay, sorry. Something strange has happened to my computer. Okay, I'll carry on.

So how is all this supposed to help consumers? We envisage that the open banking would allow in new people with new -- who would be able to offer new services. We weren't sure, again, exactly what they would be, but we could see what a

liberalization of the market could bring about.

Just as an aside, I'll say that at the time we were asked why, if we wanted to get open banking started, we wouldn't run a campaign to promote open banking. We said we didn't think that would work because that would be kind of like promoting electricity in the 19th Century. I mean, you're trying to -- it's a struggle to describe what it was, really, as most people wouldn't understand open banking.

And in the course of describing what it was, people would eventually say, well, do you mean it could actually kill me? There were risks involved. So we said, no, we wouldn't do that. So that was the third kind of unusual thing in this remedy that we didn't specify exactly what the applications were going to be. We just said we can see some examples of things that we think would be great, and we picked occasionally.

The first was sweeping services. These are services which would -- basically, if you had too much cash in your checking account at the beginning of the month, it would take that money -- the app would take some money out of your account and put it on deposit and guarantee you would get a better rate than your

bank is giving you.

If you were running a bit into the red at the end of the month, then rather relying on the bank overdraft, the app would pay money into your account and guarantee they would charge you less than your bank would charge you. And all of this would be hands-free. You would need to do nothing. This would take over the management of moving your money about. And that would be a very big threat to the banks in the UK because the most profitable customers are those who leave large balances in their current account and who run up big overdrafts. So that would be very important.

And there are a whole raft of other examples that we can see particularly for customers who you could describe as challenged in some way or vulnerable. That's been a very fruitful area of app development.

So just briefly, where we got to two years in, two years after the first API traffic started? Well, in the first -- in July 2018, which was the first quarter when all the banks had the APIs running, API call volumes in the month of July 2016 were about two million. In August this year, they were 450 million. We're cumulatively now up to about nearly 5

billion, 5 billion API calls, and the number of active users of open banking has gone through the million mark. It's approaching one and a half. It’s going up toward -- in the direction of two.

And adoption has been very, very strong in the SME section. SME is just to say adopted mobile phones first, fax machines first, everything else first. Yeah, they've adopted Open Banking first because it integrates beautifully with their cloud-based accounting systems.

All the major banks have introduced Open Banking apps. All of the banks -- all the remaining banks, including the challenger banks, they’ve done the same. They weren't compelled to, but they have done the same because it allows them to comply with PSD2 and the software is free, so they found out.

And we have, I think, 700 providers of Open Banking services now enrolled under the banking implementation entity. So there's a huge amount of activity that's taken place. And today we have not had one material security event. No data has gone astray as a result of open banking.

So the jobs aren't finished yet. Implementation should be completed next year, and people are considering whether there's a read across

from open banking to open finance and then to other areas, which I think is something I don't think you are interested in. So we're not quite there yet. Implementation should be finished next year. It's something that, oddly enough, the UK has led the world in. I'll stop there.

MS. WHITE: Thanks.

So, Professor Barr, here in the U.S. we don't currently have an open banking requirement like in the UK. But can you give us a little background on any efforts in the U.S. to require or encourage portability of financial data?

MR. BARR: Sure, Kate. And thanks for putting this terrific panel together. As you said, the U.S. is really quite far behind on this measure. I think it's important to start with thinking about why we want open banking or portability in finance.

One of the most important things is that these kinds of measures can help empower consumers to have better control over their own financial lives. We're trying to empower consumers so they can take better control, make better decisions, better access their finances, and that will help them get ahead in life and spend more time doing things that they care about, taking care of their family and the like.

A second major reason we want portability or open banking is to enhance competition. And greater competition can help drive down costs and improve services. As Bill mentioned, there's a lot of profit, for example, to be made by banks in contingent fees, overdraft fees, insufficient fund fees, and other kind of “gotcha” fees. And it turns out, as Bill said, that consumers don’t really switch bank accounts. And one of the reasons they don't is because it's hard to do.

And I think if you had better competition in financial services, it would reduce the ability of financial services firms to have these high-cost contingent fees. It will improve the ability of the incentives on banks and nonbanks alike to provide better financial services. So that's the basic frame of why we care about these issues.

In the United States today, we don't really have a coherent framework for dealing with these issues. There's screen scraping going on. There are private contracts on a bilateral basis for direct data feeds. But there's no coherent policy framework. There's fragmentation in the market. There's no real interoperability.

The private sector is beginning to get

together to try and come up with standards, but there's no government policy framework that requires them to do that and no kind of guiding hand to that effort to get them to reach agreement. And there's significant reasons why banks and other providers don't want to necessarily reach agreement on interoperability or portability, and that's hampered the development of this area.

There are no common rules about security protocols. There's a patchwork of privacy laws in the United States that affect this sector. And even in finance and banking, per se, the Gramm-Leach-Bliley Act privacy protections are quite weak. Decent protections on liability allocation for security breaches, but even there there’s significant holes in that framework.

So our basic, you know, framework in the U.S. on liability allocation, on privacy, on security, on interoperability, on open banking, we lack a coherent, strong framework, and that's really left us behind and hurt consumers and small businesses a great deal.

When you look around the world, it's not just the UK we're really far behind. The UK Open Banking system is terrific, but there’s been progress

in many countries around the world. Singapore's made huge advances in this space; India has made significant advances through their IndiaStack program; if you look at what's going on in Australia. More recently, California has its own new privacy rules, sort of a California version of the GDPR. But we at the federal level lack that coherent framework.

There is the ability to take action here under existing law to at least begin to shape up a regime that makes more sense for the United States, and it's from a provision that I worked on when I was in the Obama Administration. Section 1033 of the Dodd-Frank Act provides the authority to the Consumer Financial Protection Bureau to write rules implementing a consumer's right to access their own information.

And when we were developing this proposal in 2009, it ended up getting enacted in 2010, so 10 years ago, the whole point was to give consumers access to their own information in a form that they could then share with third-party providers so that they could get better control over their own lives and make better choices about what products and services made sense to them.

That provision has not been enacted with

rules. It's a self-executing provision with respect to the right. Consumers have that right, but there are no rules that have been written under it to actually effectuate that. And that's led to this incredible hodgepodge of activity I described before.

So I think we could start right away in the United States by having this Consumer Financial Protection Bureau implement rules so that 1033 is not just a principle; that it actually lets consumers get access to their data, lets them share it safely and securely with third parties, and lets those third parties use them to provide better services to consumers. I think that will enhance competition, it will enhance consumer autonomy, and we can get started right away under existing law.

MS. WHITE: Thank you.

So, Bill and Dr. Rucker, I know that your organizations have spent years getting your respective requirements implemented. I was wondering if you could tell us what aspects of that process were the easiest and what were the biggest challenges.

Can we start with you, Bill?

MR. ROBERTS: Yeah. Well, the easiest is easy. Having spent a long time designing the process so that we could minimize the conflict between the

parties over the agreement of the standards, that was actually the easiest part of the entire process, that very quickly consensus emerged on the standards, because there are international standards for these things. So if the standards -- the international standards that we adopted for APIs were the FAPI standards, the financial API standards. We adopted OAuth 2.0 and ID Connect for security and for authentication purposes. So that was easy, unexpectedly easy, the technical side of things.

The more difficult side, the bit that caused us the problems, was to do with those areas where we kind of left the decision for the bank, where we left it in a competitive space, if you want, for what they were to do.

So, for example, the authentication journey, this is the process whereby you are sitting down, you are talking to a personal financial management app, and you tell the app that you want it to take a look at your bank data. So it sends you off to your bank, and you say to your bank, I wish to authorize this intermediary to take a look at my bank data. This is happening in a fraction of a second.

And then your bank will put you into a process where you go through maybe 14 click-throughs,

you get a one-time password texted to you by somebody or you get a call from a call center who wants to know what the maiden name of your last dog was, and there are a lot of obstacles that seem to be put in there, to find their way into the process there.

We probably wasted -- probably the last six months on that process before we realized that, yeah, you need to have a secure process, but security doesn't always imply friction. So we basically began looking for another authentication journey, which were frictionist but secure, and we found it in basically mobile apps whereby you authenticated yourself biometrically rather than passwords; your secret questions or whatever. And that worked tremendously well when we switched to biometric authentication.

One provider’s response rates, or the abandonment rate of authentication, just disappeared and shot up through the roof. So we were expecting difficulties with a technology. They did not emerge. We weren't expecting difficulties over authentication, and whether by accident or design, they did, and it took us a little while to sort them out. But they are now sorted out.

MS. WHITE: Thank you.

Dr. Rucker? Dr. Rucker, I think you’re on

mute.

DR. RUCKER: Sorry. Once the Cures Act was in place, I think, you know, the two big things that took us actually a couple of years in rule writing, besides the whole U.S. rule writing clearance process, which you may be familiar with for folks who are students of how regulation is done in the U.S., I think there was sort of one area that was a bit more inside ball game and then one that played out publicly.

The inside ball game was really in the information blocking. As I mentioned, you can set an infinite price for an API. So how do you balance the costs of the API? And where we came down is that the use of the APIs, so an application program interface to get the data from your doctor or your hospital's medical EMR product, electronic medical record, electronic health record, that was free to the patient -- free, of course, actually being as with many other federal rules, it's part of the provision of care -- it's not free; it's just bundled into the provision of care.

Then came the delicate thing that the providers needed to then buy software to provide these application programming interfaces. And, you know,

they would provide that from their electronic health record vendors who then had incumbent status on the provision of that so that the -- and there have been various behaviors of some of the EHR vendors that were problematic.

And so we had to put in sort of, you know, costs reasonably incurred and some considerations around that so that the providers had a chance to get these application programs and interfaces, something that reflected reasonable costs, reasonable profit margins. And, conversely, the electronic medical record vendors also need incentives to build software and to build APIs.

So that balancing was a very complicated, heavily lobbying activity. And I'm proud, I think we have a reasonable pro-public balance that respects everybody's interests and moves the country forward there.

The other area that obviously the FTC has also been involved in is the whole issue of privacy, right? We don't have, as has been pointed out in your prior session, you know, we don't have sort of the GDPR kind of equivalent in the U.S., and so what are the privacy protections for third parties as patients move the data?

In HIPAA law, while there are many ways that providers can share data with payers, analytic firms, claims clearinghouses, all kinds of other entities that are part of what you sign when you just go to a doctor's office, if you will, what we're talking about here is the patients' individual right of access. And so once they have that data, they are in ownership of their version of the data and can do with it whatever they want. There's no further provider obligation. So arguably you can have an evil app, and that evil app could then, you know, do bad things with the -- with your private medical data.

So putting in a number of protections there, working with the FTC to have it sync up with the unfair business practices that the FTC has enforced on other internet properties, and allowing the providers to make that very clear, those efforts took a lot of time to get a good balance there. So that was the external part.

MS. WHITE: Thanks.

Dan, what have been the biggest challenges for companies when they’re trying to implement the ONC rules?

MR. HORBATT: Similar to what Bill and Dr. Rucker were mentioning before, a lot of it comes down

to authentication and identity management of the patients as well as the vendors who are holding their data.

In a lot of these situations, these are very much trust-based ecosystems where you have a number of different disparate parties sharing data amongst themselves, and so it's important that there's a framework in place such that Company A can specify, hey, I have credentialed this patient, this is their identity, and passing that along with any requests for any information to Company B.

And as part of this, having federally mandated levels of assurance of that identity, it is important and is really critical to ensuring that this trust network is able to be stood up and utilized. And so without that, everything more or less entirely falls apart.

So with it, mostly it seems to be getting along the lines of identity assurance level two, which is, I believe, an NIST standard, is the de facto standard right now and what we're trying to push everything to and what we're trying to coordinate on across the industry.

So as part of this -- sorry, I lost my train of thought there for a second. But, yeah, identity is

important here because medical data is one of the most sensitive pieces of information about a person. And it's not just relegated to just you as the individual. If there's a genomics component to it as well, this extends to anybody who's directly related to you as well.

So being able to know for sure that when I ask for John Smith at 123 Main Street, date of birth -- given date of birth, that I'm getting the right person's records and that there's no possibility of getting somebody else's records, especially if we're handing it off to a third party on behalf of that patient who is not necessarily a covered entity and has not as many obligations under the HIPAA privacy rule to actually maintain the sanctity of this data, is hugely important and something that we're thinking about quite often.

And the other aspect of things is the actual quality of the data itself. When moving to electronic medical records, there still is a lot of wiggle room around how that data is represented. There are different coding systems for the same conditions, different names for medications that need to get reconciled, even just different units of measure that are used across.

And being able to take all this information from various source systems and combining it into one view of a patient that can be easily reconciled at whoever's providing the treatment at that particular moment is also critically important.

And with the latest changes to push everything to FHIR, we're moving very much in the right direction where we've standardized a lot of these things, although there are still a lot of these edge cases and points of expensability that are resulting in discrepancies between the various source systems that are slowly getting reconciled.

So it’s definitely going in the right direction. We're definitely seeing a lot better standards getting pushed out. And thankfully FHIR, the Fast Healthcare Interoperability Resource, is getting pushed globally. A lot of different other countries are using it a lot. I know that they’re using it a bunch over at the NHS and other countries as well.

So we're getting to the point where interoperability isn't just a U.S. concern. It's going to be just a worldwide concern as well. And we're slowly but surely getting there to a point where we're able to speak the same language of data across

the various institutions and eventually across different countries as well.

MS. WHITE: So you say we're slowly getting there. Is there anything that can be done to help get there faster?

MR. HORBATT: I mean, I think we're doing everything that we can right now. Specifying specific versions of these standards to use, like, I believe TEFCA is specifying FHIR version R4, is great. And once the industry gets comfortable with that, we can continue to make iterative progress on standardizing further and further along those lines.

So you've got to start somewhere. We've had great success with HL7v2, moving to the clinical document architecture now to FHIR, all of it steps in the right direction. And I'm sure that we will continue to make progress along there as well. It's just unfortunately a matter of time. Nothing changes overnight. And we're discovering all sorts of new problems and edge cases with everything that we introduce, just the nature of progress.

MS. WHITE: Dr. Rucker, have you heard a lot of these -- about these sort of authentication challenges, and have you guys at ONC been giving thought to ways to help with solutions?

DR. RUCKER: Yeah. I mean, I think everybody who has data and, frankly, everybody who's on the internet, anyway, even if it's for advertising purposes, you know, wants to identify individuals for any number of business reasons.

Obviously, as Dan pointed out, in healthcare, robust authentication is pretty critical to doing it. I'm an optimist that the market is actually going to take care of these things, see. The combinations of the technologies and the richness and the ability to corroborate data sources is really advancing at an extraordinary rate.

In healthcare, there are a number of people who have advocated the government should have, you know, another government identification number, right, on top of the Social Security number, or your driver's license number or your Medicare number. All of those numbers tend to have some very deep issues, too long to go into here, but have some deep issues.

What we're finding is, as people do the richness of data, that the authentication becomes quite good. So for example, Surescripts, who manages almost all of the electronic prescribing of prescriptions in the United States, right, so they have a big authentication issue that they have to

solve. They do it with a combination of technologies. So some of that is just matching, you know, age, zip code, what is a demographic match. But they actually build up reference databases underneath, so they sort of know who moves with whom, when households move, who are family members, who are twins, so a number of these things.

So the net of that is they're getting extraordinary high match rates when you do that, and that's one entity. But if you look at all credit bureaus, claims, clearinghouses, a whole number of other players in healthcare and, frankly, in the financial service industry, are quite good at authentication. The apps that can visibly authenticate you when you deposit a check on your smartphone, we've had discussions with some of those vendors, and they tell us they're authenticating based on up to 5,000 data points, right? So that's the profile. On your smartphone, they can't just be spoofed away by getting the smartphone's electronic identity and somebody who's in cahoots with somebody at the cellular phone vendor.

So there are all kinds of authentication technologies. They're moving very, very rapidly. So I think this is a problem that will eventually lead

us, as Bill pointed out, to much higher levels of consumer convenience and power of these opening rules.

MS. WHITE: Professor Barr, are there similar concerns about authentication in the financial sector, and are there any -- is there anything that could be done to address the concerns there?

MR. BARR: There are always concerns about authentication. There are concerns in terms of limiting the potential for fraud. There are problems today with the creation of synthetic identities.

And beyond the issue of fraud or abuse in the system, the current methods we use to authenticate identity can impose very high costs on the financial sector and on consumers, and that tends to limit access to the financial system, oftentimes for those who need it the most.

So low-income consumers, immigrants, those who are sending money abroad or receiving money from abroad, the authentication costs in the system cut off access for all kinds of people who are quite low-risk for things like fraud or money laundering or terrorist financing.

So our rules for authentication are not very good at catching bad guys and are particularly good at imposing costs on the system that limit access. So

there's enormous progress we could make on this.

I agree with Dr. Rucker that there's been a lot of private sector innovation on authentication using multifactor authentication, biometric authentication. All these measures could make significant progress for us at lower costs and with better results than the system we have now.

I think what we need is we might not need the government to innovate in that way, but we do need to government to set standards for what's acceptable so that the private sector, so a bank, can rely on those in transactions and know that the government believes that the authentication is appropriate.

The government can also use those same authentication procedures to move money more quickly and more efficiently. We saw in the financial crisis and again in the pandemic that when the government wants to move money quickly to people who need it, it has a hard time doing that. And part of that is deep inefficiencies in the U.S. payment system, part of that is the lack of real-time settlements for retail payments, and part of that is the really not very good standards we have for authentication of identification.

So I think if we make progress on this front, we can help the government help people in times of crisis; we can help banks make payments; we can improve access to the financial system for people who need it the most; we can expand the ability to send money abroad, to send remittances at much lower costs; we can open up channels for remittances in countries right now that are cut off from the financial system because of identification and authentication concerns having to do with money laundering or terrorist financing.

So if we make progress on this front, we can dramatically improve the efficiency of the financial system and promote financial inclusion at the same time. I think it's a critical area to be working on.

MS. WHITE: Speaking of financial inclusion, we were talking earlier -- in the earlier panel we had someone from India who was saying that, you know, one of their -- the impetus for their sort of data portability initiatives is to give more people access to the financial sector. Is that something that -- are there consumers in the U.S. who are sort of outside the system, and could data portability help them?

MR. BARR: Yes. I mean, in the United

States, we have a significant number of people who are unbanked, who don't have access to the banking sector or had access before and got out of it because it was too costly.

And we have quite a number of people who are -- you could think of as underbanked, who need to rely on a range of alternative financial services because the formal sector doesn't serve them well. And the costs of this are really quite extraordinary for -- again, for people who can least afford it.

We've set up a system that works really well for upper-income individuals but not one that works well for lower-income individuals or even middle-income families. We need to have a financial system that really is designed at its heart and that begins with, what does the consumer need? What do individuals need to be able to manage their finances better? How do they -- how can they receive their income, store it safely, and pay bills at a much lower cost?

And our payment system really isn't set up well for that. If we made advances in this area, identification, authentication, which we talked about, a requirement for realtime payments, which is technologically feasible but in the United States has

been held back because, oftentimes, banks make a lot of money on overdraft, which is linked to not having your money right away.

We need a real-time payment system that actually works for, supports consumers. We need an identification system that opens up access. We need low cost products and services that are safe for people to use. These are all things that we can achieve. They're not -- there are technical issues in them. I don't want to say there aren't any technical issues, but the primary problem is not a technical one. It's do we have the policy and political will to create a system designed to actually serve people.

MS. WHITE: Thanks.

My next question is actually for all the panelists, which is, you know -- we've got about 20 minutes left and we've already gotten a lot of questions. So I'd like to, you know, get to a few of them. But I wanted to ask all of you if you could tell us a little about what you see in the next three to five years, like what's on the horizon for portability? You know, will we see an increase in consumer adoption? Will we see more products entering the market?

Let's start with you, Bill, or we could --

MR. ROBERTS: Sorry. I couldn't get the question. We had audio breakdown there.

MS. WHITE: I was asking what you see in the next three to five years on the horizon for the open banking, do you see increased consumer adoption? I know you've already seen a lot of it. Do you see more competition in the marketplace?

MR. ROBERTS: Yeah, I'm sorry. You broke up completely then, Kate.

MS. WHITE: Okay. Have I been unmuted? I got accidentally muted by the host. Can you all hear me again?

Oh, good. Dr. Rucker, how about you? Can you tell us what you see on the horizon in the next three to five years? Oh, no. Now you're on mute.

MR. BARR: I think I've managed to unmute myself. So maybe I'll start us off while everybody else figures their computer system out as well.

I think there's an incredible need to see greater improvement in this area in the next few years, and I think that there's a huge consumer demand and there's huge demand for small business, which we haven't talked about as much. These kinds of initiatives can really, really improve the ability of small businesses to operate efficiently, to be able to

process payments efficiently, to be able to do their business at much lower costs.

A lot of small businesses really spend a lot more on the frictions of finance than they need to, and that's because we have the wrong policy framework in the United States. We need to develop a framework that really is rooted in serving people and in serving small businesses. We need real-time settlement systems; we need information authentication systems; we need a portability requirement implemented under the framework that we potentially have; and improvement in security and privacy.

As I said, these are -- there are technical issues there, but it’s really basically an issue of political will. If we can get the political will, then in the next few years I can see a dramatic increase in portability, a dramatic increase in efficiency in the financial system, more competition in empowering consumers to have more control over their financial lives. We can get there if we have political will. And we've seen that in other countries in the world, in the UK, in India, Australia, Singapore. We can get there, but we have to make the choice that we actually care about it.

MS. WHITE: Thanks.

Dan, are you able to tell us how you see the next three to five years going?

MR. HORBATT: Yes, I would love to. So from what I have seen so far, I believe that the process of utilizing a person's individual electronic medical records is going to become a much more seamless process. We're already starting to see this with a variety of different platforms acting as stewards of the data on behalf of the patient. So the patient owns the data. It's just these various platforms that are helping to connect the dots for them.

And we're seeing this already with Apple Healthcare. You're seeing this with Google Health and Particle Health, my company's platform, as well, where patients aren't even going to necessarily need to know all the details of what's going on. They're just going to be getting better, more seamless care, faster.

They're going to be able to leverage a large cohort of applications to provide very special care to them, especially for chronic conditions. People who have chronic, ongoing conditions are going to be able to get care 24-7 through these applications that don't necessarily even need to directly involve their care team except at very specific touch points.

And, overall, I believe that there's going to be a much better increase in the efficacy of these treatments, as well as very rich data, being able to go back to an individual's care team to see how exactly they have been going, like have they been adhering to the medications that they've been on, like how are things going, without having to ask them to remember everything that's happened over the past month for them.

So data being used for patients on behalf of the patients without the patients needing to actually actively do anything for it.

MS. WHITE: Bill, do we have you back? What do you see on the horizon in the next three to five years?

MR. ROBERTS: I think what I see is the application of data portability and information sharing applying to a much larger number of areas. So I think you will see it applied beyond financial sectors into what we would call the regulated sectors, too.

I think the big question in my mind is where the big digital platforms will move, whether the big digital platforms will move into, say, the payment area, and whether the banks, maybe the big European

banks, will start moving in the opposite direction; whether they will say to themselves, you know, we need to reinvent ourselves now. It isn't just your money you need to keep safe these days; it's your data as well. So all the banks, certainly in Europe, thinking about whether they would provide a vault, not just for money, but for data as well.

One of the most peculiar, strangest things I've seen in the last 12 months was a conversation with banks in Beijing where the banks in China were lobbying the Chinese government to be given a level playing field with Alibaba, basically, because they envy the power that Alibaba has there.

So I think I see people moving into other people's spaces. I don't know where the big digital platforms will go. I don't know where the banks will go, but they seem to be moving closer to each other, where the device manufacturer will go, I can't tell either, but everybody seems to be moving to everybody else's space right now.

MS. WHITE: Dr. Rucker, what do you see on the horizon?

DR. RUCKER: Yeah. You know, I think there's a lot of interest in moving health to a more continuous 7-by-24 type of activity rather than, you

know, the intermittent go-to-the-doctor type of thing that we've historically had. And so I think, you know, the device we carry on our body pretty much all day long is obviously the logical thing to portal for that.

There are several hundred thousand, by reports, apps and app stores on things like health and fitness and exercise that don't have access to medical data. So I think there will actually be a number of apps that, having access to medical data, especially for the folks who are sicker, for the folks who have chronic illness, will be able to engage in much richer experiences.

I think these experiences are going to be fueled on the one hand by technology, which, you know, we've seen this in the rest of the app economy in the entire, you know, bricks versus mortar, mixes of bricks and mortar that everybody's experimenting with, and that same paradigm holds in healthcare. And we're also seeing it in the internet of things.

So, you know, Apple just released pulse-ox on their smart watch. I think there's one or two other brands have pulse oximeters on their smart watch. So there's an enveloping technology out there.

The other issue that is big out there, I

think, is that the markets in the U.S., transparency both on clinical care and on price. The President's had, you know, a number of policies obviously in both areas to increase transparency. That will come together with the individuals bearing more and more of healthcare costs as corporations, you know, do less and less of the shielding of those costs from the public.

So I think there's going to be a lot more consumer sovereignty demand based on just the shifting economics. You put the technology, the shifting economics together, I think we're going to see an explosive growth in, you know, the involvement of healthcare mediated via the smartphone.

MS. WHITE: So we've gotten several questions today about consumer adoption, and so it's sort of two questions. The first one for any and all of you is, what can we do to increase consumer adoption to make them more comfortable with adapting technologies that are giving them the ability to port their data?

MR. BARR: I mean, I'll just jump in again. It depends on having the policy framework. You know, right now, again, in the United States, we don't have the right policy framework to advance this. So people

are using either screen scraping or these bilateral directive data feeds. And until we have a coherent policy framework that looks out for consumers -- and that we could do based on the CFPB's current authority -- I think we're not going to have the kind of adoption that people eventually want to see once we have those protections in place.

DR. RUCKER: Yeah, if I can give the healthcare version of that, I think we do actually have in healthcare, but I agree with Professor Barr. On the financial side in healthcare, I think we do now have the policy framework. We have a robust set of, let's say, starter rules, starter data elements, and a pathway to get those.

I think a lot of it goes back to our earlier discussion of just raw convenience. People have -- you know, we're all busy, we can't remember 5,000 passwords. You know, we're overwhelmed by technology, by technology choices. So I think we naturally gravitate to things that have lower friction costs.

So the background work on -- all the background work on infrastructure, as Dan mentioned, data quality, that makes these things more elegant and explanatory to patients. And, frankly, I see the issues around authentication and informed consent,

probably two of the bigger ones we don't have in the U.S., you know, as elegant consent policies. So we do it with a sort of jury-rigging approach that basically works, but it's a high-friction approach, as, again, Professor Barr mentioned. So I think that's, in fact, a great role for the FTC, frankly, is to think about consent policies as well.

MS. WHITE: Dan, do you have anything to add about how we can increase consumer adoption?

MR. HORBATT: I think the appetite is there. As soon as the apps get out there, I think that you're going to have a lot of consumer-driven downloading and using of those apps, potential for the prescription of apps, tying together with a very robust, wearable economy as well. So things like the Apple Watch, similar other wearable devices being able to feed information back to care teams, I think is going to drive a lot of that going forward as well.

MS. WHITE: I've got a question from the audience, and it suggests that there might be some consumer confusion where they don't -- and I think we alluded to this before -- where they don't understand sort of the protections that follow the data when they move it. Is there anything we can do to sort of help with that, for anyone who's got an opinion?

MR. BARR: I think, you know, issuing some clarifying guidance under the Gramm-Leach-Bliley Act by both the FTC and the bank regulators, it might help. I think there is some confusion about -- among some about whether GLBA protections apply outside of banks. They do, but I think that making sure people understand that might help in a modest way in advancing privacy protections.

MR. HORBATT: I think -- just to jump in here as well, I think giving individuals visibility into where exactly their data is going would also drive a lot of desire to be informed in part of the process. So as a patient, if I were able to see everywhere that I currently had outstanding HIPAA authorizations for myself, that would be a very enlightening experience. It would answer a lot of questions and perhaps could even freak me out a little bit based on, you know, I don't remember giving this consent four years ago; I should probably revoke that at this point because I no longer have a need of their services. So just being able to know that you have the rights under HIPAA and being able to exercise them would drive a lot of consumer confidence, I believe.

MS. WHITE: And what about, Bill, if you can hear us, you had mentioned, yeah, when we talk about

sort of consumer adoption and sort of how can we make sure that consumers understand what they're giving consent for, how have you guys dealt with that in the open banking, making sure that consumers sort of understand what they're consenting to if they want to use your services?

MR. ROBERTS: Basically through just trying to make it clear to people through some kind of a dashboard that they know and are clear about what -- who they're giving permission, authorization, for what purposes, for what data, and over what time period, and also that they are occasionally required to reinstate that -- that authorization so that it doesn't just lie there and it can be used until it's switched off. The customer will periodically be required to say, yeah, okay, I'm okay with that data still being used.

There are issues. We are facing issues over the onward sharing of data because it isn't now just a matter of an intermediary dealing with banking -- open banking. We now have third parties handling data between the bank and the intermediary, and maybe fourth parties or maybe fifth parties.

So it kind of -- it's all of the final pieces in the implementation that we're trying to

crack to make sure that it's plain to the customer to whom they're giving authorization and for what, and that they can revoke or vary that consent through something as simple as a dashboard.

I think the only other point I'd make is that one of the two other lines of defense, if you want, that we have are the accreditation of firms who are allowed into the ecosystem. It's quite a big part of protection to ensure that their systems are as required.

And then certainly on the payment side, we have a very simple method of redress, so if things do go wrong, if data does go astray, if somebody moves money as a result, then it's pretty simple to figure out where the consumer goes, and it's strict liability. The customer goes to the bank, the bank makes the customer whole, and then it sorts it out with whichever other party to the transaction it would claim was at fault.

So we haven't cracked that yet. It's a huge issue. It's tied -- authorization is tied in heavily with issues of authentication, and I don't think anybody has an A grade on that yet with jurisdictions that we've looked at.

MS. WHITE: Well, thank you all. This has

been -- we've just got another minute, and I just wanted to thank you all for a great conversation. This has been incredibly useful and informative. And so I thank you again. And, so, our next panel will be Reconciling the Benefits and Risks of Data Portability, and that will begin at noon. And thank you all for watching.

RECONCILING THE BENEFITS AND RISKS OF DATA PORTABILITY

MR. QUILLIAN: Good afternoon. Welcome to Panel 3, Reconciling the Benefits and Risks of Data Portability. I'm Ryan Quillian, one of the Deputy Assistant Directors of the Technology Enforcement Division in the FTC's Bureau of Competition.

We have a very accomplished group here today who is going to explore this important topic. Before I briefly introduce the panel, please note that their full biographies, which tell you much more about their distinguished backgrounds, are available on our workshop webpage.

Now, our panelists. First is Ali Lange, who is a public policy manager at Google. She is based in the company's California headquarters and works closely with its Data Portability Product Team.

Pam Dixon is Founder and Executive Director of the World Privacy Forum, a public interest research group focused on consumer data privacy issues.

Next is Gabriel Nicholas, a research fellow at NYU School of Law, whose work focuses on tech competition and the politics of software.

Hodan Omaar is a policy analyst at the Center for Data Innovation, a research institute focused on the intersection of data, technology, and

public policy.

And last but certainly not least is Peter Swire, who you heard from this morning. Peter is the Elizabeth and Tommy Holder Chair of Law and Ethics at the Georgia Tech Scheller College of Business, where he teaches cybersecurity and privacy. He is also senior counsel at the Alston & Bird law firm.

We're going to do a Q&A discussion among the panelists. If we have time at the end, we will do our best to answer some questions from the audience. So please send those to dataportability@ftc.gov. You can also follow us on Twitter. The FTC will be live tweeting the event using the hashtag #datatogoftc.

Ali Lange is going to start off by telling us about Google's own data portability project, called Takeout, and the Data Transfer Project, which is the collaboration among several large technology companies.

Ali, take it away.

MS. LANGE: Thanks so much, Ryan, and thanks to the FTC for organizing this event. We're really excited to be here and share a little bit about our work on data portability.

So Google has been working on data portability for more than a decade, actually starting

back in 2007 when a team of engineers in our Chicago office had developed an early iteration of data portability tools that allowed users to export copy from individual Google products. And then four years later, in 2011, we launched a data portability product called Google Takeout, which is a centralized place for users to download their account data -- a copy of their account data.

And since then we really just continued to invest in this product and innovate and make this feature practical, easy to use, make sure it's responsive to the use cases that our users are requesting in terms of their needs for data portability. And a lot of folks have talked a lot about what data portability is, so I think we can assume folks understand, but just sort of for some context on how Google has implemented it, the Takeout product actually currently allows users to download machine-readable copies of data from over 70 Google products, in addition to making that data accessible through their Google account in general.

So through this process, users can select the data format that they want to use, depending on the product, the type of data they want to download, what they're planning to do with it. So, for example,

a user connects from their Google Docs from drive into a .docx file format if they're going to use it with Microsoft. So as you're going through the Takeout process, if there's an industry standard format that's available, we pre-select that for export. But when you're going through, you have the option to change that to whatever file format you'd like from the options that are available.

We've also in recent years made it increasingly available for users to transfer data directly between a Google account to another service that they can authenticate into. So, for example, rather than downloading that drive file onto your computer and then reuploading it into Microsoft OneDrive, you can send it directly if you can authenticate into your OneDrive account without downloading it onto your computer first.

We've also added other features in recent years for Takeout, including options to schedule recurring exports, and we're expecting to add more features. We're always adding more features for the portability tool.

As you're using Takeout, one thing that's important and is made clear in the flow, is that it's not deleting the data from your Google account. It

creates a copy that you can use, you know, to have a backup, to sort of get a bird's eye view of what's in your account or move that data to a different service, as we described.

The Takeout functionality is also -- I'm sorry, the deletion functionality is also available in your Google account, but it's on a separate page. If you're going through the deletion flow, it does actually direct you to Takeout to see if you want a copy of your data before you delete your account. They are linked in that way.

Throughout this process, Google has implemented really strong privacy and security protections for Takeout to guard against unauthorized access, diversion of data or any other types of fraud. So, for example, in earlier panels there was a discussion around authentication. But for Takeout, users have to re-authenticate their account to execute a download, even if they're already signed in. And that would include two-factor if they have that turned on in their account. That's a protection that we have installed for our Takeout users.

So after sort of a decade of work on data portability, we have made a lot of improvements as we've described, and we sort of have learned a lot of

information about what users expect, how things are working, what types of functionality is the most useful.

And over that time, one of the things that we really focused on is, as I mentioned, making the data easier to move directly to another service. And one of the challenges that we found along the way of doing that is that that one-to-one connection takes quite a bit of engineering effort, right, to connect the APIs to every other service you might want to download your data to or sort of transport a copy of your data to.

So as we were working on that project, we really thought there was probably a way to make this easier, particularly given that the direct transfer is such a significant improvement in user experience, but the engineering effort can be a little bit challenging for folks. And that was really the core insight that we built the Data Transfer Project on.

So we founded the Data Transfer Project in 2018 based on these insights around, you know, the challenges that we faced around direct service-to-service portability and really wanted to make that an easier thing across the industry. The Data Transfer Project is an open-source data portability platform

and it enables people to transfer their data directly between online services. It's essentially an industry effort that we continue to lead with partners at Apple, Facebook, Microsoft, and Twitter. And this effort is really designed to address some of those technical challenges and help portability scale and be practical.

And, in particular, it's addressed to help reducing -- or it’s designed to help address the engineering effort that each individual company has to put into direct service-to-service portability. So the fundamental concept -- and I would direct folks who are interested in more of the technical details to our website, which is datatransferproject.dev.

So the fundamental concept is really that there’s a system of API adapters and common data models that are built through the open-source community and available on GitHub. Anybody can contribute, anybody can sort of see the code and evaluate it. And these adapters and data models, they facilitate the direct transfer between providers.

And so by sort of centralizing this engineering effort, by making it open source and available for others to participate in, the concept is basically that you're making it much more scalable for

other companies to participate.

So to give a sense of what this improvement to scale is through the Data Transfer Project, you can sort of imagine a world in which there are 10 companies that offer, like, a photos product. For each of them to all be interconnected, they would have to build 90 connections. To be maintained, each company has to do nine different connections and maintain those and sort of make them operate. And each time a new company comes into the space, you have to build a new one.

So with the Data Transfer Project, instead of building that sort of one-to-one web of connections, things go through a centralized model where you have a sort of conversion process. And so all you have to do as an individual company is maintain your storefront, essentially. You have to maintain your adapter into the project. But you don't have to maintain and worry about all of the other ones. So it really just reduces the amount of effort folks have to put in, which is the key element of the scalability of the project.

We really hope and believe and have seen early evidence that this effort will enable innovation. We want users to be empowered to try out

new services and experiences. We don't want companies to have to be worrying about being integrated with, you know, N-squared providers. Portability is something that companies can look forward to enabling and not sort of dread having to deal with. And the Data Transfer Project is really a way to facilitate that and make that a little bit easier so that innovation can grow and thrive based on this process.

Importantly, throughout the Data Transfer Project, we've spent a lot of time grappling with the privacy and security kind of elements of the project. And, again, there's actually a pretty extensive analysis of this in our white paper and in the comments we submitted to the FTC, that include, for example, a table of various responsibilities for all of the stakeholders in the transfer process, sort of how we think -- you know, who's responsible for what. But fundamentally, even though portability does provide a significant benefit for users, there's an important element of users being able to move their data safely, maintaining strong privacy and security assurances along the way.

So from our point of view, providers on both sides of the portability transaction need to have strong privacy and security measures such as

encryption in transit and other features to guard against any sort of fraud or other concerns that a user might have. They should be explained to users. Users should understand the practices of, for example, their destination of their data so they're clear on what is going to happen. And, like I said, this is detailed pretty extensively in our white paper and also in the comments to the FTC.

So as I mentioned, fundamentally, DTP is helpful for folks who want to try a new service, and portability is helpful for folks who want to try a new service. But one of the main innovations of the Data Transfer Project is that it’s actually really helpful for individuals who are operating on slow or metered connections; people who are on mobile devices in areas without access to high-speed internet or where internet is very expensive.

So if you’re thinking of portability in the sort of original conception where you would download your data and then re-upload it to a new service provider, that's a pretty expensive thing to do. You really have to have a personal device that has a fair amount of storage. You're talking about using a lot of bandwidth to download and re-upload the data.

So for folks who are based in the U.S. or

Europe, this may seem sort of like a marginal change, although not for everyone but for some. But for folks around the world, this is actually a really significant difference. You're shifting the infrastructure burden from the individual to have this pretty extensive infrastructure back to the company so the data is moving through the cloud, and they're not taking on these kind of expenses basically of literally moving it. So that's something we're feeling really positive about.

Just quickly, I know I'm sort of running over your time limit, Ryan, but in addition to the partners on the project who I listed, Facebook, Microsoft, Twitter and Apple, several companies, developers, individuals, have made significant contributions to the implementation of DTP since it launched. So we just want to thank everyone who has participated, not only in building the code, but also participating in building kind of understanding and having conversations with us and thinking through some of the issues.

More than two dozen contributors from a combination of partners in the open source community have inserted 168,000 lines of code and changed more than 85,000 files on the GitHub website. So it’s been

a pretty significant effort in the community, and we're really grateful for all the work folks have put in.

If you're interested in getting involved or interested in becoming part of that community, there's details on the website, which again is datatransferproject.dev. I'm sorry, I think I might have misspoke earlier, datatransferproject.dev. And you can learn more about kind of what the partners are doing. We post periodic updates and we have some explanations on there on how people can get involved, no matter where you are, if you're an individual developer, if you're just a thought leader interested in participating.

So that's basically the history of Google's effort on data portability, not only making it sort of easy, practical, you know, really working in our own platform to make sure folks have what they need to move their data and to feel like they have sufficient access and visibility, but also to really contribute to a broader effort across all of the ecosystems to make data portability practical and to enable this direct transfer which we really see as the future of data portability.

MR. QUILLIAN: Thanks so much, Ali. We

appreciate that overview.

I'm now going to turn to the rest of the panel to give us some more background on themselves and their work in the data portability space, as well as describe their perspective on why data portability is important.

Gabriel, can you please give us a little background on your interest in this area and tell us, you know, from your perspective what the goals of data portability are.

MR. NICHOLAS: Sure. And thank you, Ryan, and thank you to the FTC for having a panel on such an important topic. I think it's really great to be sort of having these conversations now.

So I see there as being two separate goals of data portability. On the one hand, there is this idea of giving consumers access and ownership over their data, either for archival reasons or for oversight. And we've seen a lot of strides in this area from Google Takeout, as Ali mentioned before, Facebook's Download Your Information tool, and sort of a number of other portability regimes that have come up after the GDPR.

The other goal of data portability can be to encourage competition by allowing new and existing

products and companies to build new platforms, build new products, based off of existing data. Now, this area is much more experimental. As I think Professor Graef said in the first panel, we haven't seen many products, if any products, built out of portability in this way, and we don't know if it works.

And so I think a great way for the FTC to look at data portability is as a big experiment in improving competition in tech. And the way to regulate it is to consider how do we best set up the conditions for this experiment so as to make it most likely work?

And in that experiment, you know, it's important to focus on the consumers, as we've talked a lot about, you know, is their privacy being maintained, is the experience secure, and is it easy enough for them to actually do -- you know, to allow them to move their data, if interested, but there's also a question from the competitors' perspective, where is the data that companies are making available enough to actually build platforms off of? And neither -- you know, neither works alone. Portability can't improve competition if competitors can't use the data or if users aren't interested in moving.

And, you know, I worked as a software

engineer at Yahoo! for about five years and I sort of got to see a little bit behind the scenes of what data it takes to actually build products, and that's what really got me interested in this area. And so, yeah, I look forward to talking more with the other folks here about sort of how we can architect data portability in order to see this sort of successful experiment.

MR. QUILLIAN: Great. Thank you, Gabriel.

Pam, what about you? What are the goals of data portability from your perspective and why is it important to the World Privacy Forum?

MS. DIXON: Sure. So for us it's really -- data portability is something that effectuates data autonomy for consumers, and that's an incredibly important thing. Of course, we saw this really take hold when the GDPR went into effect. And there have been some interesting results from that.

But our interest in data portability, beyond just the autonomy aspects, is also some of the privacy risks. And we'd really like to see some changes in some of the areas, particularly around health data. And I'd like to talk more about that later. But for now let's just earmark that as a definite privacy risk with data portability.

Also, we're very interested in the identity ecosystems that are being built up, and in some cases, identity silos that are being built up in order to authenticate individuals who want to port their data. So these are both very interesting privacy issues.

I do think that there are solutions, and it's very clear that there are solutions. It's just that they're not always implemented at this point. Thanks, Ryan.

MS. QUILLIAN: Thank you, Pam.

Hodan, why don’t you give -- what do you view as the goals of data portability and what is the Center for Data Innovation’s interest in this issue?

MS. OMAAR: Thanks very much, Ryan, and thanks to the FTC for having me. I think the goals of data portability, in addition to the pro-competitive market efficiencies and access goals that Gabe talked about, is also an opportunity to create innovation opportunities that kind of help create new products and new services.

So we know what the issue is. We know that some companies unfairly restrict access to data, but data portability can kind of tackle this by creating evidence, where there is evidence-based problems, where it can identify that it can create solutions

that are sector-specific, and really where it can balance the costs of data portability regimes against the benefits to overall consumer welfare.

And I think where it can create competition and empower consumers is really speaking to the competition goal. But, also, where it's able to move firms and the economy at large away from how can we collect data and how can we store it to how can we use it and how can we analyze it, really speaks to that innovation goal.

And the Center for Data Innovation is concerned with how data can be used to benefit consumers, increase consumer welfare, and help the economy and society at large. And that's really where I think our interest in data portability and this issue really comes into play.

MR. QUILLIAN: Great. Thank you, Hodan.

Peter, I enjoyed your introductory overview this morning. It was very comprehensive. But is there anything you would like to add at this point about how we should view the goals of data portability?

I think you're on mute, Peter.

MR. SWIRE: Sorry. I have four very, very quick points. The first is there's a goal of

research. If we move data to different places there might be various kinds of research that work better than we did before. And that could be data from the public or private sector.

The second is, as one of the goals around competition, all of the case studies turned out to have an aspect of lock-in about it so that if everything is unlocked and open, you don't have to write a law to open up the windows. But if there's a lock of some sort, that's when mandates to open up things tend to be important. And so for competition goals, looking for lock-in turned out to be more important than I would have thought before we looked at the case studies.

The third point is I don't think we've heard the word "multihoming" yet today, and it's a word that comes up often in these portability discussions. That's the idea where maybe you're using the first service and you like it, but you start to like to also use the second service or the third service. You don't have to leave the first service. Portability might let you do some things on the first service and do some other things you like on the second or third service. And one way you get competition and innovation is if people start to have multiple places

they call home and not just one place they call home.

And the last point for the goal for having a data portability regime is to try to figure out when somebody says security and privacy, is it a pretext or is it real? So I think we've heard in the UK, in a banking context, the antitrust officials were thinking that maybe the banks were using cybersecurity as an excuse or pretext not to do Interoperability, and then with some hard work, they were able to build intraoperability. And interestingly today, the regulators said there have been no material security incidents.

So having a way to detect what's a pretext, what's a good reason to be careful for privacy and security, might help us decide when the best opportunities are for having portability. Thanks.

MR. QUILLIAN: That's really interesting. Thank you, Peter. And let's go a little deeper into some of these issues surrounding data portability and how it may affect competition.

Ali, can you give a sense of how consumers are using the data they download through Takeout or port or download from the Data Transfer Project? And as you're going through, if you could include a description of the categories of data that consumers

have access to and those that they do not, that would be really helpful.

MS. LANGE: Yeah, happy to. So as I mentioned, Google Takeout currently allows users to explore a copy of their data from over 70 Google products. After users do that, we obviously have no visibility into what happens next, and so periodically we'll ask people through surveys, you know, what they're planning to do with this data. And that's really our core insight into how data is used. This is a difference between data that's being downloaded and re-uploaded or downloaded for another purpose compared to data that you might transfer directly. So I just wanted to give some background on kind of how we have some of this information.

So those 70 products include a lot of products where users are storing data in their account, things you would think of like emails, documents, photos, everything like that. And that also includes things like search history, YouTube watch history, other things you can see in your Google account that you can download a copy of if you wanted to explore them or move them to another service or use them for some other purpose, for some research purpose or otherwise, which we've seen folks sort of do some

research on their own browser history or things like that, which has been really cool.

But basically, since launching Takeout in 2011, which was the second iteration, a second iteration of our portability tool in general, Google users have exported more than an exabyte of data from Google products, which is a lot, a lot of data. Part of that is because some of the more popular products for folks to download are actually photos, which are bigger file sizes. So -- but an exabyte, it is a significant amount of data for people to download.

And, actually, right now, there is currently an average of about 2.25 million exports a month, and over 200 billion files were exported in 2019. So there's a lot of different ways you can count, you know, what's being moved, how is it being moved, and that gives you a sense of, like, the volume of the data in total as well as sort of the frequency of using the tool and how many files there are, which is a pretty good spread of information. So it's very popular. Folks are definitely taking advantage of the service that we provide.

Takeout is part of the Google account, which is linked directly from basically every single one of our products, so if anybody is on Chrome right now,

you might see a little icon in the corner with a letter of your name or a picture. If you click on that, you can easily get to your Google account, and in your Google account, you'll find Takeout, as well as any other services you need to manage the data that's in there. So we're sort of moving it as proximal as we can, your account, to the services that you're using with Google to make it easy to access that and use it.

So as I mentioned, we do sometimes take these surveys, what are people planning to do with this data that they download their Takeout. Actually, we've found a wide variety of use cases that portability supports, all of which have been referenced already on this call, and, in particular, I heard a reference on the regulatory call from Mr. -- I can't remember his last name, I'm sorry, from India, who referenced the idea folks are downloading a copy of their data, which I think is a really good way to describe it, right? They might not be trying to leave a service or switch a service. They might be trying to do something new, which is also the concept Peter just referenced and the idea of multihoming.

So when we've seen folks downloading data, sometimes they're downloading data from an individual

product because they do want to try a new feature on a different product. Photos is a really good example of this. People will download photos, they might want to upload it to a different service that offers a different kind of functionality, they might want to share it with a different person, they might just want to have a copy. So that's another place where we really put a lot of effort into enabling that direct transfer, probably because those are fairly considerable file sizes, and we know it's a common use case for people, so we want to make it as easy as possible.

So we actually recently just implemented some new features in the fall that allow users to directly export their photos to Flickr and OneDrive, in addition to Dropbox and Box. So we have a pretty robust set of places folks can move their photos.

Users also sometimes want to download their data to create a backup. They just want to have a copy on their local device. If they want to -- they feel better having a copy around. That’s a use case we hear reported. And sometimes folks are exploring the data that's in their account, something we see periodically reported through blogs or the news or things folks are curious what’s in their account. It

allows them to make changes to their settings and do some adjustments where they feel they want to make any changes to what's stored there.

You had also asked about what we've seen through the Data Transfer Project. Since the July 2018 sort of announcement and launch of the project, in addition to significant investment in the open source protocols sort of in the GitHub repository, several of the partners have launched product features that are powered by DTP. So, as I mentioned, last fall, for example, Google announced -- I'm sorry, launched a new feature that enables you to move your photo library directly to Flickr or Microsoft OneDrive. And this includes album selection. So it can be individual photos, all your photos or specific albums.

Facebook also recently had some new announcements enabling users to move their photos directly to new services. So they had offered Google previously in the year and now they've added Dropbox and -- I'm sorry, I'm going to say this wrong, but I think it's Koofr, which is a European cloud storage company. So Facebook has some good features that they've offered as well through data transfer.

Twitter and Apple are sort of testing and

building and planning to roll things out in the near future. And Microsoft has released an open source log-viewing tool for Office 365 enterprise customers that's built on DPT technology.

So basically in addition to all of that work, one of the things that the Data Transfer partners are doing is trying to build awareness of the product and sort of encourage more folks to participate, to greater facilitate those involvements.

So, for example, Google has presented a demo of MyData even as far back as 2018, showing how you can move cat photos between two services, sort of a classic internet participation process.

So, again, DTP is an open source project. Anyone can establish a usable format or translate from existing ones and they'll immediately become available for everybody. So we're expecting to see a lot more development on DTP in the coming months. But those are the current implementations and those are some of the things that we've seen on Google Takeout as far as what folks are interested in doing and the best way to make that -- sort of facilitate that for them to make it work.

MR. QUILLIAN: Great.

Hodan, the comment submitted by the Center

for Data Innovation notes that data portability can increase market efficiency, but in some cases, it will not encourage competitors to create more innovative products. Can you expound on those concepts? And in particular, are there particular market dynamics or types of data that would lend themselves toward increasing market efficiency?

MS. OMAAR: I think markets are most efficient when consumers are best informed, when markets are most transparent and when firms are best able to innovate with data. But the issue is, in some sectors, the incentives of who holds the data and the incentives of the data subject can differ greatly.

So today we talked about utility data, and so -- and because of the kind of economic models, utility providers can want to reduce overall energy consumption to save money. And, for me, that's great. I, too, want to lower my energy consumption to save money, so our incentives are aligned. But in other cases, like we heard in the last panel, in finance and in healthcare, those incentives can be really different, and the greater the discrepancy between incentives and the greater the need for data portability.

So I think where we can make data available,

that kind of works toward the market dynamics we want to see. So more market transparency, more informed consumers, and like Peter said, where we can have multiple economic agents using the same data rather than having to replicate it, we will move toward overall market efficiency.

And I think that's a more useful framework to think about what types of data might help market efficiency, rather than kind of creating an exhaustive list of all the different data types and the variabilities within those data types. Because data is -- data isn't like any other economic asset. It doesn't have value in and of itself. Its value really comes from the context in which it's being used.

So I think where we can kind of balance how data is being used to improve those three things -- market transparency to help promote competition, to fuel choice engines for consumers so that they can make the optimal choice for them, and to help firms really focus on using data rather than storing it and collecting it -- will help us kind of move toward overall market efficiency.

MR. QUILLIAN: Great. Thanks, Hodan.

And, Gabriel, building on that, from a competitive perspective is the data that consumers can

download or port under the existing data portability initiatives, is that data competitively significant? Like, in other words, could a competitor use the data that consumers port to develop products that compete with existing companies?

MR. NICHOLAS: Yeah. So I think it's a great question. And I think it is -- as Hodan was saying, it's not necessarily the same answer in every sector. But we do see a number of sectors, including finance, including agriculture, as one of the FTC comments talks about; auto dealers per Peter Swire's work, where there are a lot of places that they're feeling like they are not getting enough data to actually build competitors or to lower the switching costs in the way that data portability promises.

And at NYU I've done some research on this case in social media where we looked at Facebook Download Your Information data and we gave it to developers and product managers and other people that we would expect to compete with Facebook and said, what can you do with this information? Are you able to use it to build products? And in general the answer was, no, because there were certain shortcomings in the data. And some of these I think are -- there are shortcomings that could be addressed

in a way that would be be useful across sectors. Right?

So some really basic things such as documentation describing what data users can expect in -- when they port. And, you know, the structure of that data; versioning, you know, so that companies can't change the way that their data portability regime looks without expecting; encrypted versions of unique identifiers so that, you know, you can tell when it's the same person or same entity across ports.

And I think in a similar vein going off of what Ali was talking about before, it’s also important for users moving their data to have a smooth experience, which I think a lot of places right now isn't necessarily that. It is the antiquated “download your data, upload it somewhere else” model. And I think shifting toward the direct transfer model is another area that could really help sort of make this data actually more competitively significant.

MR. QUILLIAN: Great. Thank you, Gabriel.

So, Peter, we've heard a fair amount today about some potential tension between the goals of privacy and competition in the context of data portability. I was just hoping, if you could expound on that a little bit from your perspective and give us

a sense of what is that tension and can it be resolved?

MR. SWIRE: Well, on cybersecurity the case study suggested three areas to look at. The first, which we've heard a lot about today, is authentication. Who is going to get access to the health data? And I think Pam is nodding her head in part because the authentication in the health care system is not very good right now. And so somebody might be able to fake and get into someone else's data.

The second area for security is security in transit. And I think there's a norm emerging that it should be encrypted when it goes from point A to point B. The trick is whether you do screen scraping or you do API, application programming interfaces. And there's been some vague calls on some of the regimes for open APIs, but actually getting everybody to connect to everybody faces the problems that Ali talked about, the 90 connections even if there's just 10 companies. So how to have standards for security in transit.

And the third area for security is you're going to need to have pretty effective standards. It sounds like a lot of lines of code in GitHub for DTP,

and these standards will have security and privacy components to what the standards are, who gets to see what, who has what access privileges, et cetera.

So those are three areas for security, authentication, security in transit, and standards, having the right stuff built in that really have to be built, and you're probably going to need quite a bunch of engineers and technical people to do that.

On privacy, the biggest risks -- well, the categories in my outline of questions are what's going to happen to identify data? What's going to happen to deidentify data because of data transfers and bulk deidentify? People might be able to figure out who it is.

There's a big issue about privacy issues about other people. So if I have a picture that I want to transfer and the picture is of a 10-year-old kid of some other family, do I have to get the parents' permission before I transfer the data? So those are some of the privacy issues.

And then the last one I'll say is what was mentioned earlier about onward transfers, which is it goes from sending company to the receiving company, and then it can go to other places, the fourth and fifth place. And what the rules are going to be for

that, does there have to be new consumer consent? Does there have to be some visibility of that for the consumer? The rules for onward transfer can make it a lot more complicated. And if you're really going to try to clamp down on the privacy and security risks, you're probably going to have to give some attention to onward transfer. Thanks.

MR. QUILLIAN: Thanks, Peter. Pam, I mean, I'd love to get your thoughts on onward transfer as well. But in addition to that, you know, data portability has been presented as a consumer right and it becomes easier to transfer that information. Is there a risk that consumers will share too much of their own data? And, similarly, are there cases in which security or privacy risks might arise after the transfer to the data recipient kind of along the lines of what Peter was describing?

MS. DIXON: I'll try to bundle all of this up. So, again, there are benefits to data portability, and I don't want to discount that. But I do have to state that there are some very significant risks, particularly in the health care sector.

So, there are short-term risks but there are very significant long-term risks as well. To just start with the short-term risks right off the bat --

and I think Peter may have alluded to this -- let's say you're signed into a health care portal and you're looking at your record.

Most portals assume you're authenticated and it's a one-click transfer. Meanwhile, when you go to make that transfer of your health data out of your healthcare portal, I've personally not yet seen a notice that explains to a patient that their data is changing from a HIPAA-protected regulatory structure to a completely different regulatory structure, which may mean none at all. It may -- it gets really complex depending on where you're transferring it to. But not every transfer of patient data -- in fact, I would wager that the majority of them are not necessarily going to another health care provider. A lot of people are transferring data for COVID research. But they didn't know that they were actually creating a situation where their entire health record was then going because that's what they transferred.

And there's such direct transfer that is frictionless within the health care context. It's literally like a one-click. So it's really important to consider something, and that is this: HIPAA does confer affirmative rights to patients. For example,

you will have the affirmative right to request something called an accounting of disclosure; who's seen your record. There are limits, but it's still important. You have the right to restrict disclosure of your records in some instances. If there's a subpoena for your records, you will be notified so you can quash that subpoena.

None of that happens when you allow your records affirmatively by that click to go outside of the HIPAA context. And I think that the number of patients who know this and truly understand the consequences of this action are far and few between. Maybe health care attorneys and privacy geeks, but that's -- that would be the limit of it.

And then we get to long-term consequences, which several of the panelists have alluded to, which is the onward transfer problem. So, first off, what we're seeing is that some people unfortunately transfer their data to fraudsters and then are subject to absolutely heinous situations that arise from that, all sorts and manners of the worst kinds of identity theft you can think of. But the other problem is a little bit less onerous but has a long tail, which is data transfers to data brokers that are posing as a health care researcher or doing market research and

calling themselves research, health research. Well they don't say that it's for marketing purposes.

But, you see, there's no rules around this yet. And as a result it's a bit of the wild west. And unfortunately when that data healthcare file, a medical file, is transferred outside of HIPAA, it's free and clear. No further regulations apply to it, save for perhaps a privacy policy that's posted on the website, which would then bring that health care file under FTC Act Section 5 or perhaps under no regulation at all.

So right now one of the things we're seeing are brand new data sets since the rules took effect this year that are just loaded with new health data. So health data is on the market now. And once this data escapes the HIPAA-protected system, it's a very, very big challenge to try to reign that back in.

Now, all of that being said, there are some very good instances of people acquiring data for legitimate purposes. They're very clear. That exists. But we're kind of focused on the risks and mitigating those risks. So, there you go.

MR. QUILLIAN: Thanks, Pam. And as kind of a followup, the data that's covered by HIPAA is at least covered by a sector-specific data privacy

regime. What's your view of efforts to set up portability rights more broadly outside the context of the universal privacy framework?

MS. DIXON: Yeah, that's a really great question. So, as we all know, the U.S. has a sectoral privacy regime. So what ends up happening is you'll have, you know, financial privacy regulation like Gramm-Leach-Bliley or the FCRA, Fair Credit Reporting Act. Then over here you'll have HIPAA and so on and so forth. For education privacy, it's the Family Educational Rights and Privacy Act. But in between those areas are significant gaps in coverage, and that's where things get really, really difficult because the moment that -- especially health data leaves the sectoral protections, those protections do not attach to the data. They attach to the healthcare provider only. And I do think that if there were an omnibus situation then it would be much more like Europe, where the protections travel along and there are fewer gaps. It's not perfect, but the gaps are further apart and much fewer.

MR. QUILLIAN: Thanks, Pam.

Peter, you covered this a little bit earlier but I was wondering, based on your experience, what are the greatest data-security-related risks from

portability?

MR. SWIRE: I tried to answer that in terms of authentication, security and transit and having the standards with good security and privacy practices built in. Maybe I can just quickly follow up on something Pam was saying about the comparison with Europe and the United States.

In Europe, there are these general rules in the background. So if it went from a health provider who might be under stricter rules to someone else, there's still GDPR in place. In the United States, if it goes from a HIPAA entity relatively strict to some other entity outside of the sector, maybe the FTC can enforce for deceptive practices, but in practice there's a much lower level of requirement. And so the risks to privacy when you don't have a national law are higher when it goes out of the sector by sector.

And then the one other point is even in Europe where they have the general background privacy rules, when they were doing their open banking and payment services rules, the lead privacy supervisor, Giovanni Buttarelli, believed that for each sector it was important to have sector-specific laws that went beyond it.

And so even in Europe with the back-end

privacy rules, the privacy experts thought there needed to be some sector-specific protections. So I think as it moves from one sector to another from a regulated entity to another, that really deserves a lot of attention in any overall policy decisions the FTC looks at.

MR. QUILLIAN: Thanks, Peter.

Gabriel, what would a data portability regime that facilitates competition by reducing barriers to entry, by example reducing switching costs, helping overcome network effects, reducing lock-in, et cetera, what would that actually look like in practice?

MR. NICHOLAS: Yeah. So, I think to your question, it's important that if data -- the approach to data portability is hoping to improve competition that I think it not just focus on user lock-in, because user lock-in is just one of many effects of this going on that make competition difficult in the tech sector.

And one of those -- and an important one, I think, is network effects that -- and I think there are ways that data portability can also help network effects. So, for example, there's the idea of group portability or collective portability wherein users

who share data might want to move all of their data together to another platform. And that sort of helps mitigate the empty platform idea of like, well, you don't want to go to a platform where nobody is. And you don't necessarily -- in some cases you don't want to go to a platform where you don't know anyone.

And so allowing, say, you know, in the social example a group of friends who are all messaging on Viber wants to move to WhatsApp, by giving them a mechanism to all opt into that and to allow them to move the data that they share together, I think can make sure that data doesn't fall into the gaps. You know, right now in a lot of portability regimes when you download a conversation that you have with someone, you only get your side of the conversation, which isn't particularly useful. And the other person only gets their side of the conversation. And even if you uploaded them together, there can be insufficient data, data that falls in the cracks, that prevents that whole conversation from actually being rebuilt. So I think collective portability is a way to address that.

I also think that there are -- it's important to be careful with the way that we address switching costs, because there are -- as someone in

the first panel mentioned, there are ways that lowering switching costs could end up harming competition. And I think this is really important when we think about data portability reciprocity, or, you know, if you import data from elsewhere, do you also have to make your data exportable?

And this is very tricky question, but there are some places where that might actually prevent competitors from using ported data. So there's the example of -- let's take the example of Salesforce, right, which is the dominant customer relationship management -- the customer relationship management platform. So, you know, they have very strong network effects. They have a lot of customers and, you know, they're very difficult to compete with.

Now, smaller places can really only compete on price. They have to offer a lower price for a CRM that does not as much enjoy network effects and does not have as many users on it. And currently switching costs for CRMs are high. You have to either pay a consultant to do it or buy an expensive tool to move the data over, and these high switching costs make sure that the small CRMs have a little bit of room to grow that they can enjoy some of their own network effects.

And there is precedence for dealing with this in the law. So the Access Act has this, which was the proposed portability law that placed a monthly active user count. And I think there's a number of ways that really should be looked at to make sure that data is flowing in the direction that we're interested in it flowing.

MR. QUILLIAN: Thanks, Gabriel.

Pam, do you have any thoughts on that topic?

MS. DIXON: Yeah. Just, you know, Gabe, I might have to call you and talk with you about this more. I had a thought, and I just realized something listening to you, which is this: The data portability types that we look at the most are data portability types wherein an entire very data-rich file is transferred all in one lump.

So, for example, financial reports that include a lot of rich data, and health files, which is, of course, reams of very rich data. So there's not this, you know, multidimensional, multiperson aspect to this data. It doesn't have to be reconstituted in order to have a lot of value to multiple types of actors. So I do think that that is an important distinguishing characteristic, and perhaps a point of risk that can be addressed by

rules, whereas if you have a complete file type that's very rich, what are the rules and notifications, et cetera, that need to be involved with that data type. Thanks, Ryan.

MR. QUILLIAN: Thanks, Pam.

Hodan, did you want to add anything about the difference in jurisdictional laws or approaches?

MS. OMAAR: Yes. So I just wanted to add on to what Pam said. I think when we think about what works in the EU and what will work in the U.S., we need to remember the real differences or just be cognizant of the differences in those sectors. So if we think about banking in Europe, the banking sector is a lot more concentrated than it is here in the U.S. And world bank data really supports that. And as someone who lives in the UK or lived in the UK and have just come to the U.S., you know, everyone I knew growing up, everyone is with one of six or seven -- you know, less than 10 banks.

But here you go to different towns, you go to different places, everybody's with a different bank, a local bank. And so really the kind of rules that we enforce on sectors, how they work in the EU how they're going to work in the U.S., has to have -- be really steeped in research and evidence-based, and

we have to think about how that might actually -- just because somebody worked in the EU, it doesn't necessarily mean that economy-wide rules are going to be -- work here or that they're going to help those smaller banks or just be effective overall.

MR. QUILLIAN: Great. Thank you, Hodan.

And we appreciate everybody who submitted questions to dataportability@ftc.gov. We have one question from the audience here for Peter. Going back to your concern about pretextual arguments against developing interoperability, is it possible to distinguish between pretextual arguments from one -- like, pretextual arguments from ones that arrive from privacy or security?

MR. SWIRE: Thanks. To me, that was one of the big questions I tried to think about during my research. I love privacy and cybersecurity. I love having competition and innovation. And you see cybersecurity and privacy being made as an argument when it might be a pretext.

So based on all the case studies, I'll tell a story from the automobile dealers case studies, and there's litigation on this and I've been an expert witness in it, but I think I can describe it neutrally. So the claim has been from the automobile

dealers that they need to be able to get access to their own company's data and move it to a different supplier and have other software help. And the claim has been made by the companies who run the operating system that that would have terrible cybersecurity and privacy problems with it, especially the cybersecurity. And so that's a fight. And there's facts about that.

So after working through all the case studies, one way you might have a guess that it's a pretext is if the company that's running things, that has the data, allows all sorts of transfers to itself and its affiliates on special terms that advantage it, but acts more strictly against outside groups. And that kind of discriminatory treatment might be a hint that it's not really worried about cybersecurity; that it's actually trying to get economic advantage.

So in antitrust law there's the idea of FRAND -- fair, reasonable and nondiscriminatory terms -- basically that you treat the outside and inside companies the same. And it turns out in a bunch of the portability laws that we have, including the HHS interoperability rule, including in the Arizona auto dealers rule, and I think there's two or three more, in Europe there's some of them, all of them -- payment

services directive. There's an emerging standard that when the company is saying, no, I can't do it because of cybersecurity or privacy, there's an emerging standard that you can apply those FRAND approaches that is fair, reasonable and nondiscriminatory.

And that gives at least a start to saying, this time it looks like they're doing it for their own advantage, or this time it looks like they have a bona fide cybersecurity point. So in my paper, which is up at SSRN, there's a fairly long discussion about these FRAND kind of approaches. And I think that's one hint about whether we trust the cybersecurity argument or not.

MR. QUILLIAN: Thanks, Peter.

So I'd like to turn now, since this workshop is a data-gathering and explanatory exercise, I'd like to get everybody's thoughts on research that's been helpful to them and things that still need to be done.

So, Hodan, do you have any thoughts on the types of research that would help us better understand whether existing data portability requirements are benefitting consumers?

MS. OMAAR: I think to better understand the extent to which data portability is helping consumers, we really need to understand how much these regimes

cost financially; how effective they actually are in specific sectors, and also the kind of risks associated with potential data breaches.

ITIF, the Information Technology and Innovation Foundation, wrote a report called “Costs of Unnecessarily Stringent Federal Data Privacy Law” that estimated the total cost of data portability requirements for all U.S. organizations that handle personal data would be roughly around $510 million. Professor Graef’s work that we heard in the first panel, her work analyzing and comparing GDPR versus sector-specific data portability regimes, has also been really useful to me.

And then finally Oxford University, James Pavur showed that confusion over data access requirements in the GDPR has led to significant security incidents with a substantial number of organizations responding to malicious data requests with approximately one in four turning over personally identifiable information.

So I think if we can quantify the financial costs and qualify the kind of privacy and security issues and really balance this against kind of evidence-based, sector-specific benefits, then policymakers will be able to better kind of create

targeted specific data portability rules that kind of are successful in increasing consumer welfare.

MR. QUILLIAN: Great. Thank you, Hodan.

Ali, what research related to data portability have you found most helpful, and what do you think needs to be done to advance our understanding the benefits and risks related to it?

MS. LANGE: Yeah, there's certainly a lot of good scholarship on potential benefits of portability. And big thanks to folks on this panel and across this workshop for all the work that they've done to really think through some of these issues and put pen to paper and describe things and sort of move the ball forward on how we think through portability. So I just want to acknowledge all that work already.

One thing that's interesting hearing today's discussion is lot of the conversation is really focused on frameworks and kind of protocols and rules for the conceptualization of portability. From our point of view, I think it sort of -- and it makes sense because I think it feels like it should be a technically simple exercise. It certainly seems simpler than a lot of other things that our phone might do, which feel a little bit like magic.

But from our point of view after a decade of

work on this, we found that portability is actually a pretty technical challenging puzzle. The favorite -- like the favorite kind that folks at Google like to solve. And so I would say that work doesn't need to be or shouldn't be discounted in the broader scheme of what work needs to be done. You know, it's not the case that if you can just solve a framework question then everything else will fall into place without that effort.

And so from our point of view in addition to that work and the actual technical engineering that we're sort of trying to advance with our partners in the Data Transfer Project or ourselves on our platform, there's a lot of judgment that needs to be made in decision-making throughout the process. So I guess the answer to your question from my point of view is to sort of think through other ways to help inform that decision-making, things about the use cases people care about, the portability actions they find useful, things that work as expected, what are expectations for people who are moving data; technical needs to make data portability practical so the work we're advancing through DTP.

We welcome more folks to participate in that to help really move that ball forward, and

fundamentally thinking through how do you keep this sustainable, right? Echoing back to some of Peter's points on the sort of N-squared problem, how do we think about things that scale successfully, how do we think about things that are useful for those folks?

So I do think there's a pretty strong set of technical questions that can also merit attention. And this is one of the reasons why we really like the open source solution space for Data Transfer Project, is to create the space for folks to come and iterate and think through some of those questions, in addition to all the great policy work that’s being done by folks on this call and otherwise.

MR. QUILLIAN: All right, Pam. Same question to you: What research has been most helpful and what do we need to do to advance the ball?

MS. DIXON: Yeah. So I think that for me the research that I'm really looking at right now and that's been very helpful has been research around digital identity ecosystems and how they interact in regards to verifying and authenticating someone and identifying who they are.

We're seeing the emergence of a lot of what I call strong identity. Strong identity requirements include biometrics. Now, that doesn't always occur,

but we're seeing more of it. So there's a rich literature on tokenization versus requiring strong identity everywhere. There's a rich literature that's emerging on how identity ecosystems are working in this context. And I think that this is a very under-researched area in terms of how it's working from the consumer's point of view.

There's a lot of research on how it's working from the business entity that's attempting to either acquire or port the data. But from the consumer perspective, what identification mechanisms are going to be required of them and how good are they? What's their quality? What's their endurance? What are their -- what are the qualities of that type of identity? Is it a biometric? Is it something else? What is it? And what are the kinds of standards we want in place for that?

So I do also think that the role of standards becomes very important here. And it can be technical standards as well as data typing standards, as well as other kinds of procedural standards.

MR. QUILLIAN: All right. Gabriel, in addition to your own publications, what research related to data portability have you found most helpful, and what's coming next for what needs to be

done?

MR. NICHOLAS: So I think there are three general -- so I do want to echo, I think that Pam and Hodan and Ali all bring up really great points that sort of do need additional research. So I'll add three to that.

One of them is I think there needs to be historical research on sort of analogs to portability. Peter has talked about before how mobile number portability, it gets used a lot, but it's sort of a bad example of what data portability looks like in the wild. I think there might be better examples out there.

One that comes to mind is the '96 Telecoms Act and unbundling where that was an area where sort of per what Hodan was saying before that, you know, it wasn't able to lead to innovation because companies weren't able to differentiate their products enough or they weren't able to compete on price.

So I think there's a lot of areas where there have been things similar to portability before that have succeeded or failed that could be brought into these conversations.

A second thing I think is important is this question that's come up a lot in this panel of general

versus sectoral approaches. Is there any kind of data portability law that really is useful across sectors and should be implemented, and what are the kind of things that need to be thought about sectorally. And at NYU Law, we're hoping to put on a conference about this sort of thing, so if this is the kind of thing that interests you, please reach out to me over Twitter or email or otherwise.

And a final topic that has not -- a sort of whole Pandora's box that we've not really opened is API portability versus one-off exports. I know that a number of comments discussed this where, you know, there's this tradeoff of API portability can mean -- it can sort of increase the number of risks, it can increase the threat to the data-sending entity, but it can also open up a whole world of other products that could be built that couldn't otherwise be built.

So I think there's a million questions around those things, around API portability versus one-off exports that need to be sorted out, and it's really an exciting area that's a wide open space for a lot of research.

MR. QUILLIAN: Great. Thanks, Gabriel.

And, Peter, to wrap up, same question to you. What's been good and what needs to happen?

MR. SWIRE: Well, first I want to say briefly why it's a hard problem. In a lot of ways it's when you open up data flows and when do you close data flows in a database society. And that's one reason that the issues sort of spread out all over the place, and I think the FTC will have to figure out how to cabin in some way in order to have its best recommendations going forward.

I'll mention three areas of research. One is a plug for Gabe's work on group or collective portability. I had never heard of it or thought of it until he wrote his article last year about it. And so if you're a set of people who like bird feeders, you know, and you want to move your comments from one place to another, how can you scale it so the groups can move to different services or competing services.

A second is there's been work done by Professor Inge Graef, who was on the first panel, and others about other case studies, after-markets for cars in the European Union; electric utility portability in Australia and the UK and the EU. And so keeping -- learning from the case study so you're not just off in theory land but you have some real examples.

And the third one -- and I think the area

for the most work, and sometimes it seems like the least glamorous work, is how to do the standards, the technical standards. We've had several people mention how much hard work it is, whether it's on APIs, open APIs, or having a clearinghouse kind of structure like DTP has, how to do the data formats so that people in healthcare are transferring the right stuff and not everything like a fire hose.

I think there's a lot more work to be done by the technical people, by the patience of working on the standards, and might be 60 or 80 or 90 percent of the work that has to get done. And policy people never want to go into a standards conversation. I've had horrible experiences in standards processes with do not track. But that's where the portability that will happen or won't happen, and so a much bigger fraction of the work should be how do we get the standards in place for secure and effective transfer, even though nobody's going to want to do it.

MR. QUILLIAN: Thanks, Peter.

So we have a question from the audience, and I will ask Pam to lead off here. Have you looked at the way that individuals can play a part in enabling the market and ensuring the fair exchange of value for the use of their data, calling out misuse, supported

by tools that enable and empower them as active participants in the ecosystem?

MS. DIXON: So if I could ask the person asking the question a little bit more, clarifying about their question, but I'm going to take two different stabs at it very briefly.

So, first, I mean, when you're dealing with data portability and you're pulling data, this goes back to something that's come up on this panel several times, which is sometimes this data is commingled. Additionally -- and that's with the data of other people that are, you know, on the platform with you, in group conversations or joint conversations, et cetera.

But there's another complicating factor, which is whatever the platform or entity put into that data, there may be analytical information that's been added and so on and so forth. So at the end of the day, you can come up with a very complex analysis that, you know, there are a lot of people that own this data. So we have a paper that we workshopped at the Privacy Law Scholars Conference, Jane Winn and I, but we haven’t quite published it yet. We will this year.

But the paper is really about common pooled

resources, a la Elinor Ostrom and the governance of the commons, and what do you do when there's a resource that is rivalrous, to use those terms, and it can be claimed by several different entities or individuals. What do you do? And there's a whole philosophy on what you do with that.

But the thing that you don't do is claim that you own it. So there is that school of thought. And I do think that this has to be looked at very carefully. This is -- we're in an active research phase on this idea. But I think it's an important idea to consider, and let's see if it has merit in this context. We're in the exploration phase. But I do think it's important to understand that it's very difficult to just say, oh, here's my health record; let me sell it to someone. I think that that can have just profoundly deleterious, unintended consequences if we start looking at monetizing your own data in that way, kind of turns into a Les Miserables where people are selling their teeth. So I just think we have to be very, very, very cautious in that area.

And because I chatted so much, I think I'll stop there. It's a great question, though.

MR. QUILLIAN: Thanks.

Gabe, did you have something you wanted to

add on this audience question?

MR. NICHOLAS: Yeah. I just wanted to add that I think the way it currently is today, this is a really difficult process to do from the bottom up, because platforms really in many industries have a lot of control over the data that they make available.

So I know that there's the example of the Light Collective, which is a patient advocacy group that's interested in, you know, taking groups where, you know, it's like you take back a conversation or, you know, patient groups with diseases, where they're sharing sensitive medical information. And Facebook has advertently or inadvertently monetized that data. And there are groups that want to be able to move off to another platform, but the data that's made available to them is inefficient. It's insufficient and there aren't legal mechanisms to get the data that would be sufficient there.

So I think this is a place where for those bottom-up initiatives to happen, there also needs to be legal support for those to happen.

MR. QUILLIAN: Thanks, Gabe.

Peter, you wanted to add something really quick?

MR. SWIRE: Yeah. This is a -- the question

illustrates where there's tension between the antitrust outlook and the privacy outlook. So when you talk about individuals enabling the market, ensuring fair exchange of value for their data, for antitrust trained people it seems natural to want to get the market to move to allow transfers to have higher value.

And as Pam said, and as many people in Europe have said, if you look at this as a privacy right that's going to be invaded and treated badly, there's a lot of people on the privacy side that are super skeptical of it. So the different discourses of antitrust people and privacy people are really far apart on this particular issue.

MR. QUILLIAN: Great.

Hodan?

MS. OMAAR: So I just wanted to add something on a rather different point. But just while we have time in this forum, I just wanted to bring up that not all data is digitized, right? Some of it is analog, a lot of it is. And when we have very kind of strict data portability regimes that apply only to electronic data, we can create these sort of kind of perverse incentives that have companies wanting to avoid digitizing their data and in some sense actually

making lock-in problems even worse, and also dampening the kind of trends toward digitization.

So as we think about what rules and regimes we want to kind of implement, that's something to think about.

MR. QUILLIAN: Great. Thank you. And so we've got about five minutes left. So I have kind of a round-up question for each of you, maybe one or two minutes in response.

We'll start with you, Ali. So where do you see data portability moving or going in the next three to five years, and are there any concerns, you know, as we go in that direction or things that you think we need to address before we get there?

MS. LANGE: Yeah, I mean, I think that the alignment toward more service-to-service portability is something I really see growing in the coming years. I think the reason for that is really fundamentally back to the core motivation for Google and the core insights that we've had throughout the process and I think that I've heard others on the panel echo, which is that making the design users to focus on what people want to do, making it useful for folks, making it practical both in terms of feature kind of expectations and in terms of, you know, the lighter

technical infrastructure placed on individuals and things like this.

This all sort of merges toward a world in which I think we'll see more kind of behind the scenes work done by the technical community, the open source community and others.

I should say I'm speaking mostly from my own sector. I think the observations others have made about the healthcare sector and financial sectors, who have been more regulated than sort of slightly different sectors. I probably have less youthful insight into that work. But fundamentally where I see it going is really more toward focusing on user-center design, making things more usable, making things more practical for individuals to make decisions about trying new features or staying in control of their data in other ways.

MR. QUILLIAN: Great, thanks.

Gabriel, do you have thoughts on the next three to five years?

MR. NICHOLAS: I guess I do and I don't, because, again, I just want to reiterate this feeling that, like, we don't -- there are some sectors that have experimented around with data portability, but by and large we don't know its effectiveness at

introducing competition.

And I hope that in the next couple years we will find out. You know, I think there's a little bit of a “if you build it, they will come” mentality, but in reality we'll build it, and we’ll hopefully build it as well as we can and hope they come. And so I'm definitely excited to see in the next couple of years what happens with data portability, what competitors end up building with it, what issues users run into it, and both how this policy adjusts to improve those ways that competitors are benefitting and add further user protections where those get trampled on.

MR. QUILLIAN: Well, I certainly appreciate any “Field of Dreams” reference, so I appreciate you throwing that in there.

Hodan, do you have any thoughts on what's coming up next and anything that needs to get corrected as we’re going in that direction?

MS. OMAAR: Yes. So I think I’d just add on to what Gabe said and say I can say where I hope to see data portability go, which is kind of increasing that market efficiency by, you know, making markets more transparent, making consumers better informed, and helping firms really be able to use and analyze that data rather than spending so much time on kind of

collecting and storing it.

MR. QUILLIAN: Great. Thanks, Hodan.

Pam, what are your thoughts?

MS. DIXON: Sure. I'd really love to see more standards work and more individuals involved with the standards work. Peter is right, people don't like doing standards, but they're going to be the backbone of a lot of this.

For example, there could be a standard and it wouldn't take 15 years to develop, but there could be a standard for notifications in the healthcare sector prior to transfer out. And this would be fantastic and it would really solve some problems. And that's the second thing I would say, is I really do think that we can reach out and get some very good low-hanging fruit that would help a lot of people fairly quickly. And I don't think it would be that difficult. I think there is some low-hanging fruit. There's some harder fruit and I think that has to do with the standards and also with the identity ecosystems. But I think that that will proceed. I would be surprised if it didn't.

MR. QUILLIAN: And, Peter, let's stick with baseball, cleanup hitter, finish us off with the --

MR. SWIRE: I'm batting fifth. Anyway, so

one thing to note is that data portability is popular. And there's bills in Congress from both the Republican side and Democratic side, and both of them include data portability for comprehensive privacy legislation in the U.S. Most of the states who proposed laws in the last two years have had data portability in them. So it's a hooray kind of term. People are in favor of portability from a lot of perspectives, so we should expect a lot more of that.

The second thing, I hope in the next three to five years, is to build on what the FTC is doing today by bringing together different sectors -- health care, financial services, digital platforms. They don't talk to each other necessarily that much. People think their own world is the whole world because each of those worlds is very huge.

Also, doing it cross nationally. We've talked about the EU today and Australia and others are doing it. So I think that if we can continue the learning process instead of thinking we're having to create it from scratch and learn from these different experiences and case studies that we're likely to have better ideas of how to do the next thing and meet some of Gabe's hopes for it actually being useful, and the rest of everybody's hopes for having privacy, security

and competition.

So I think, you know -- I'm a professor. Further study will help. And I think this workshop is a very big step toward doing that.

MR. QUILLIAN: Well, great. Well, in response I'd just like to thank all of you for participating today. I think this has been a really great discussion, in addition to the other panels, which I found really interesting. It's a complex topic and there's a lot more to do. So I appreciate your time and all your thoughts.

We're going to take a short break now and reconvene at 1:30 Eastern for our final panel, which will focus on several key concerns confronting data portability initiatives: namely security, privacy, standardization and interoperability. So stay tuned and thanks, everybody.

(Brief recess.)

REALIZING DATA PORTABILITY'S POTENTIAL:
MATERIAL CHALLENGES AND SOLUTIONS

MR. BROWN: Welcome back. Thank you for joining us for our final panel of the day, Realizing Data Portability's Potential: Material Challenges and its Solutions.

My name is Jarad Brown. I'm an attorney in the Division of Privacy and Identity Protection. On this panel, we will further discuss some specific topics that have been raised throughout the day: privacy, security, standards and interoperability, as well as possible solutions.

If we have time, I'll try to incorporate any questions we receive from viewers. So please send any questions you have to dataportability@ftc.gov.

I'd like to introduce my panelists. In the interest of time, I'm going to keep to very brief introductions, but I highly recommend you read their full bios on the event page to learn more about their impressive work.

First is Erika Brown Lee. Erika is Senior Vice President and Assistant General Counsel at Mastercard, where she is the global lead for the company's privacy advocacy efforts, including cybersecurity, and led the team that provides guidance

and ensures compliance with privacy and data protection laws across the company's products and services.

Next, we have Sara Collins. Sara Collins is Policy Counsel at Public Knowledge, focusing on privacy, data and platform accountability. Public Knowledge is a public interest advocacy organization with a mission to promote freedom of expression, an open internet and access to affordable communication tools and creative works.

Next is Bennett Cyphers. Bennett is a staff technologist at the Electronic Frontier Foundation and works on the tech projects team. EFF is a nonprofit organization working to preserve and enhance civil liberties in the digital world, promoting privacy, free expression and innovation online through activism, technology, products, law and policy.

Next is Michael Murray. Michael co-founded the Mission:data Coalition in 2013 and serves as its president. Mission:data advocates for data portability in the power sector in order to promote energy efficiency and reductions in carbon emissions.

And, finally, last but not least, is Julian Ranger. Julian is Executive President and Founder of digi.me, a decentralized personal data solution

that is operational today.

Thank you all for joining me today.

Let's get right to it. We've got a lot of interesting topics to talk about.

Sara, if I could ask you to get started. I'd like to talk about privacy first. And can you tell us a little bit about Public Knowledge's work in the area of data portability, and then also kind of describe some of the privacy concerns data portability may present, in your opinion.

MS. COLLINS: Thank you, Jarad, and thank you to the FTC for having me here today. So to think about data -- think about Public Knowledge as our work in data portability, it's important to think about our values, which is open access to the internet, free expression. So data portability for us is a mechanism to either promote consumer welfare, to improve competition in the tech space. So we look at data portability as a tool. It's a means to get to an end we're looking for.

So in that case, we want to make sure any data portability regime or scheme protects the privacy of users. We already know from privacy work -- I mean, if any of you have been following this in the day-to-day, that privacy harms are running rampant.

We have seen loss of opportunity. We've seen -- we've seen economic harms. We've seen all sorts of harms arising from privacy violations. So when we evaluate data portability, we think about it in a sense of, one, is it giving consumers autonomy; and, two, does the scheme that's being proposed sufficiently protect privacy and sufficiently do that in a way where consumers can trust that when they share their data they're only sharing it for the purpose of trying a new service or moving their data to a service that better meets their needs.

MR. BROWN: Thank you, Sara.

Erika, can I turn to you next? Could you talk about data portability at Mastercard and how are you thinking about privacy, both for existing data portability requirements you're under as well as future proposals?

MS. BROWN LEE: Sure. And, thanks, Jarad, for putting this great panel together, and to the FTC for hosting a day on this important topic. So as a technology company and a payment network, Mastercard doesn't actually issue cards, credit cards. That's done by our customers, who are the banks. And we do have a product and take a very consumer-centric approach with respect to privacy and our practices.

And so if I could start by just talking a little bit about those because they fit into our discussion.

Last fall, we launched what we call the Data Responsibility Initiative, which is grounded in four principles. First, that consumers, individuals, own their own data. Second, that individuals control their data and have the right to understand how their data is used. Third, that individuals should benefit from the use of their data. And, fourth, really is from a security prospective in that individuals data should be protected and used responsibly.

So data portability is really about, for us, we think about giving individuals more control over their data. And it's an important tool and a way in which that really makes sense with respect to the expectations that individuals have around their data. And ideally when it works data portability has that potential to not only open up possibilities for consumers, but to enable business innovation and competition.

And so at Mastercard we have a consumer-facing, public-facing portal that we call the My Data Portal where any individual can go to make a request to access their personal information and then receive

it in a portable form.

In terms of just the current legal requirements, we've heard a lot today about the existing regimes, including GDPR and the CCPA, both of which have certain limitations with regard to scope in terms of, you know, what data portability applies to.

And really with respect to those laws and any privacy laws, it requires companies to do a very deep assessment in terms of what the data they have is and how that data is maintained in order to be able to comply with privacy laws, but the difference with data portability law requirements is that technical aspect, because you have to do a sort of deep assessment from a technical prospective of how to make data available.

With regard to future laws and some of the proposals that are on the table, you know, we see various legislatures across the globe contemplating different, you know, ways of addressing data portability. You know, they're not necessarily homogeneous, though, and so there is that potential for divergence, which then would, you know, potentially affect the ability for companies to provide that data in a portable way.

And this goes toward that point that we've heard about a lot today with interoperability, which

is the key to creating an environment that is compatible not just within an industry but across industries so that the principles that we see around data portability are consistently applied, even if there are sectoral differences.

And then I'll just wrap up by saying that as part of the conversation there should be consideration of the ethical factors in terms of how we think about data portability. And it's not so much just whether you can but whether you should port the data. So I'll pause there. Thanks, Jarad.

MR. BROWN: Thanks.

Michael, if I could turn to you next, could you tell us a little bit about your background and work in energy sector data portability, and then how does privacy come up in that space?

MR. MURRAY: Thank you, Jarad. And thanks to the FTC for holding this. This is a really great workshop today. So, Mission:data is a nonprofit coalition of about 30 technology companies that provide energy management services to homes and to businesses. Many of you may be familiar with the use cases around banking and healthcare that have been talked about so far today, but you may not be familiar with the use cases in the energy sector.

So let me just give you a quick example. You may have heard about the blackouts that occurred in California about five or six weeks ago. There were some record-breaking temperatures that created a supply crunch; power went out for just about a couple of hours. And one of Mission:data's member companies has turned energy conservation into a game that sort of directly helps keep the lights on in California.

So if you save energy in your house, for an hour here or an hour there, you can earn points that were redeemable through the software application for cash or gift cards. And in aggregate, there were over 100,000 households participating across the state. They delivered several hundred megawatts of demand reduction to the California wholesale power market and literally helped keep the lights on for millions of Americans.

So the way that this works is that a demand response aggregator, as we call it, gets the customer's permission to share usage data that's held by the electric utility. And once utility provides the usage data, the aggregators goes to the wholesale market and says, you know, energy usage across this fleet of homes, you know, was X, and then I intervened, and now it's Y. And so that delta X minus

Y is what you get paid for for delivery by the wholesale market.

And so consumers win. They get a share of that revenue. Costly power plants don't need to be built, and we can use this demand flexibility to increase the amount of renewable energy sources on the grid.

So data portability for me is really important among electric utilities because of climate change. I don't know about you all, but we've been living in smoke out here on the west coast ever since Labor Day. It's one of the warmest summer on record and unfortunately it's probably going to be the coldest summer for the next 100 years. So this is something that really concerns me.

And data portability is tricky in the electric sector because we have over 3,500 retail electric utilities. Some are regulated by states, some by municipalities and some by cooperative boards. It's a diverse patchwork and it makes it very difficult to establish standards, whether we're talking about API standards, informed consent standards or privacy standards.

So as for privacy, I have always believed that I think you can be both pro-privacy and pro-

customer choice at the same time. Incumbents, the utilities in my case, often inflate the real privacy risks. And we heard a bit -- a little bit about this earlier in the day. Some privacy concerns are, of course, very legitimate, but others are exaggerated and I think serve some pretty nakedly anticompetitive purposes. With residential energy usage data, there are Fourth Amendment search issues when law enforcement is involved. We absolutely understand that. However, if a customer wants their information shared and it's opt-in, it's really untenable these days for a utility to say, you know, no, we're not going to allow that. And so the debate in the energy sector really hasn't been should a customer be able to share his or her data, instead it's about the method, about how that's accomplished both in terms of technical exchanges, API standards and most importantly the user experience issue and whether the user experience is -- you know, leads to fully informed consent.

MR. BROWN: Thank you, Michael.

Julian, if I could turn next to you, your company is a solution for porting data between numerous services. Could you tell us a little bit more about that and the other work you've done in this

area and then give us the thoughts about how you're thinking about enabling data portability without undermining privacy.

MR. RANGER: Certainly. So at digi.me, we use data portability today both explicit and implicit, because it's not everywhere. I'll try and explain why and how. So the most important thing is that all of the future capabilities we as citizens, businesses, governments and society are looking for actually require us to share more data and better data as individuals, not less. We can't do a lot of the future things without sharing more. So we have to find a way that's private, secure and consented.

And an obvious example is precision or personalized medicine where I may need to share my health data since I was born, my advanced wearables, my genomics, the food I buy and eat, even my social data is a good indicator of my mental state.

But how do I do that? I can't. How can anybody get their hands on that because it's all locked away in different data silos. And even then, how do I control it? And that's where we come in as what's called a data facilitator, or my data operator, as your librarian and your postman, and to do that fully privately, fully securely and with consent.

So we enable you to get a full copy of your data. And we're just like an email program in many ways. You download an email program to your device, authenticate your 2-3-4 email channels and then a miracle happens, all your data is there. Well, it's the same with digi.me. You download digi.me, you connect to your various sources of data, and we've got health and bank and wearables and media and social. You authenticate and then your digi.me gets a full copy of your data, normalizes it, and then you choose where to store it. So you choose. It's all fully encrypted with your own encryption. So you actually end up with a full copy of your data. Nobody else has it. Nobody, not any of the big five, have as much data as you end up with yourself. And it's 100 percent private because only you have it. And it's fully secure because it's all encrypted with a key held only on your device, so fully decentralized.

So now the other thing that we do then is provide a full consent stack enabling any business or service to ask you for elements of that data for a value exchange that you agree with and that might be different for lots of different people.

And if you say yes, your digi.me extracts just the data that's covered by the consent

certificate and passes it securely to the Apple service, which actually may be fully on your device. So your data doesn't have to get repromulgated around the universe. Imagine most of the things can be done. My diabetes service can be on your device, or the bank service can be on the device.

Now, it's really important that that value exchange, because you received your data by data portability, but then when you pass it on, it's dependent on -- and I use the words from GDPR, explicit and informed consent. And so we use the certificate that's been designed over many years to meet that bar and actually exceed it. And it says explicitly what the data will be used for, whether it will be processed on a device or taken off a device, whether it will be shared with third parties; if so, who and why, and more details including your ability because you own the data now to actually see the data you're going to share before you share it.

And then, most importantly, because we're really worried about reuse, of course, but that certificate is a legal contract. If the receiving party uses the data other than as stated in the certificate, then it's a breach of contract law, in addition to any privacy breach. And that's -- the

penalties are significantly harsher.

So if we actually look at it, we can actually meet all of the future requirements for data exchange by not thinking about data going from Company A to Company B, and so on and so forth, all those complications, but just straight to the individuals. Now, we're one of the world-leading data facilitators. There are others. And you bring the data to the individual who build the best composite view of all of their data and over time, and then shares it when companies ask for them and the data can be local. So if we look today -- and I mean today -- we enable U.S., European and Australian citizens to aggregate more data on themselves and to subsequently share it than any company has today, including the top five.

So if you think Facebook and Google and Apple have a lot of data on you, you can have more data yourself today. So effective data portability exists today. But as we'll discuss as we go through this session, we can and should do more.

MR. BROWN: Thanks, Julian.

Bennett, if I could turn to you next, could you talk about your work and your organization's work in data portability, and also address whether we have the solutions, in your opinion, for other privacy

problems data portability can present, or are there outstanding questions about how sort of get to yes on data portability?

MR. CYPHERS: Sure, yeah. So the way EFF looks at data portability is, I think, through two separate lenses. The first is as like a user rights issue and as a user control issue. And so just kind of at a bare minimum people who generate data, people about whom data is generated and stored by companies, should have the rights to see, to download, to manipulate, to use that data however they want.

The second lens is competition and innovation. And so as a lot of people have already said, there are competition issues where large walled gardens can get access to tons and tons of data from tons and tons of different people and then use that -- monetize that data, use it as sort of anticompetitive cudgel against their competitors, and kind of act as jealous dragons sometimes sitting on top of their data hordes and refusing to share it with their users or with other smaller companies who would like to use it for other things as well.

And so data portability can go a long way -- data portability mandates and good data portability standards and practices can go a long way toward sort

of chipping away at those monopolies and making the marketplace more competitive and more innovative.

So in terms of the challenges associated with data portability, I think there are some privacy issues with -- around, like, forcing companies to make data portable, for opening up laws so that small innovators like digi.me and their friends can do more to extract data on users' behalf, but for the most part those issues are just sort of microcosm of the privacy issues that we already face.

As Sara was saying, the world is not a private place right now. There's a lot of data flowing around, and the vast majority of the time, I think, users don't have enough control or knowledge about what's happening with their data already, and so data portability might in some cases sort of bring attention to or exacerbate the existing privacy issues with the internet today. But I don't think it's going to create many new privacy issues. And a lot of time I think, like, the idea that a user being given access to their own data is going to create more privacy issues than, like, the status quo where data is being collected and shared about users without their knowledge or consent much of the time. It is a little bit -- it is often argued in bad faith by incumbents

who benefit from data not being shared enough.

And so I think Sara is going to talk about this more later, but our perspective is generally that we need good general privacy laws. User need to feel like they have rights to access their own data and that when companies are using their data to provide them products or services, those companies have certain responsibilities to handle that data in a way that is going to benefit the users.

And so we look at it as there's a general privacy problem and data portability brings attention to that problem, but we need to solve the bigger problem.

MR. BROWN: Sorry. Thank you, Bennett. And actually I'll redirect this to Sara, which is I'd like to open up a similar question to other speakers, you know, what are the privacy solutions that can help us with the data portability challenges or do you think there's too many questions here? And, Sara, could you take that first?

MS. COLLINS: Yeah. So, yes, definitely. We need comprehensive federal privacy legislation. And there's a couple of major benefits not just to portability but to the digital ecosystem at large.

First, we need something that makes sure

consumers aren't exploited for their data. This makes the internet ecosystem better. This also makes it easier to port for a couple reasons. One, you have a set of minimum standards about how data must be treated by all parties involved in a portability schema. Two, it removes a pretextual reason for a larger incumbent who may not want to share data for an anticompetitive reason to then share data.

Right now, a platform or a large competitor might look at the U.S. landscape, know that they aren't really covered by any privacy rules and say, frankly, I don't think I can open up APIs because I'm not sure my data -- this data will be safe. And that's a reasonable argument at the moment, or at least it is supported by the facts on the ground. If you remove that argument, you now have another reason or one impediment left to data portability.

One other thing I'd like to flag and something Public Knowledge has been thinking about is creating explicitly a digital regulator. And this regulator would act as a neutral arbiter for some of these pretextual reasons we've been hearing about. Peter Swire brought this up in the last panel. But a digital regulator with expertise, technical expertise, that can really make decisions sector by sector on

what data is needed to make portability worthwhile, is something bigger like interoperability needed; how these different markets work together, are so important to really getting an ecosystem that's safe and also respects consumers.

And just a final point I'd like to make, we've been hearing a bunch about, like, consumer consent or understanding of risk. And I don't particularly love that framework. I don't think consumers should be expected to understand each app's privacy policies and pros and cons. I think a reasonable expectation is that people are going to act with your data reasonably; that they're not going to do harm with it; that they're not going to exploit it.

And so I would love to see a regulatory and statutory ecosystem that supports that belief that consumers already have. We know people aren't going to read privacy policies because frankly they're unintelligible to nonlawyers. So let's do away with the fiction and let's create a system that creates the benefits of data portability while it also minimizes the privacy risks that Bennett's brought up.

MR. BROWN: Thank you. Before we switch over to other topics, I wanted to see if any of my panelists wanted to follow up on Sara and Bennett's

thoughts.

MR. RANGER: Yeah, just a quick point because I'm very much of the opinion that data portability actually reduces the privacy risk because it doesn't come in on its own, and it shouldn't come in on its own.

So if we look at GDPR, it came in with the explicit and informed consent. So you crack down hard on the tracking stuff which you're not consenting to. Now, GDPR does have three or four other uses when you can use data, and they're fair. But all of the illegal use, as we would say in Europe, of the data needs to be cracked down on. So therefore the way in which you get data is from the individual who gets it from data portability.

So actually data portability, which at the end of the day, even for all the big companies together, means that everybody can access more data and use more data. Right? But it's counterbalanced by that explicit and informed consent.

And, Sara, you talk about people don't read terms and conditions, and they don't. But that doesn't mean, say, you can't have a clear consent certificate. You just have to put the work into it. And we have and we've done it with Kantara Initiative

as well, and it is clear. And we've got years of evidence to show that. You can show people, but what you have to want is to make that your whole reason for being; that you want to make it clear for people. And if you want to make it clear, and therefore if you're a digital data facilitator, which is our whole role in life, then just like you want to make the electricity safe if you facilitate bringing electricity, you can make the sharing of your data safe and you can make people understand it.

But I just wanted to make the point that data portability comes with explicit and informed consent as the safety net.

MS. BROWN LEE: Yeah. And I just wanted to add, I mean, I think that that's really correct. And, you know, to your point, Sara, about the idea of privacy, you know, is not having as much, I think it really does come down to an issue of trust. And if data portability can be used in a way to enhance that trust, I mean, putting aside some of the security issues separately, but just from a control perspective in that, you know, we want to be able to port your data, to exercise control over your data, trust that you will be able to get your data from companies or from organizations, and then be able to exercise

control. I think that's really a good starting place.

But you can't really do that, I think, toward Julian's point, without having information about it. It has to be informed consent. And so you have to have that access base to be able to get the data and then be able to exercise control, which I think addresses some of those concerns about misuse or not having knowledge or awareness of how an individual's data is being used.

MR. BROWN: Thanks, Erika. And if I could unfortunately go right back to you, I think we need to switch over now to security. And I will say to the extent my panelists, if there's a thought that I didn't give you a minute to ask, I will not be too frustrated if you want to sneak it in as we talk about these other topics which I know have some important overlaps. But let me switch now to the topic of security concerns and actually turn right back to you, Erika, as I said. Could you kick us off by talking about the security concerns, some of which we heard earlier in the day, that data portability efforts can really introduce.

MS. BROWN LEE: Sure. And, I mean, I think all of these topics are related. Security is that critical pillar of data portability. And so, you

know, and certainly for us, you know, it's part of our commitment with respect to data practices. As you mentioned, Peter Swire did refer to some of the pieces of security and how they come up. And so, you know, building upon that, it certainly, for us, comes up in the aspect of -- well, first for authentication and verification of the request itself. The financial services industry certainly has a lot of experience in preventing and monitoring and detecting fraud, and so that's really crucial in terms of the security piece for any data sharing circumstances.

But it goes back also to a point I raised earlier, which is understanding the type of data that you have and that would be part of what would be provided to individuals is critical because from a -- you know, from a corporate perspective, operationalizing the security piece requires an understanding of the different types of data so that you can build in those security steps and appropriate verification steps as part of that process.

And so, you know, the consumer-centric or individual-centric approach ensures that really from the start that the transfer and the port of data is coming from a place of consumer or individual requests and making sure that it's not only at their request,

but also for their benefit.

The second part that really comes into play, of course, with the security piece of data portability is the transmission itself. And so, you know, there are certain regimes that do talk about the types of mechanisms to ensure the security in transit, the guidance around the GDPR, from Article 29 Working Party Statement mentions encryption. That's something that has been raised in other panels. And so that's an example of where you see, you know, protection of data that's in transit.

I do think that it is important when you talk about security that you address that flip side, which is what happens if it doesn't go right and, you know, liability is triggered. And so thinking about the norms for how liability is evaluated is a bit more complex because we were talking about -- or it was mentioned earlier in other panels that there is sort of sectoral approach and very different approach in different jurisdictions. So not just, of course, with GDPR, but for financial services, the Payment Services Directive, or PSD2, is one of the sectoral laws that also comes into play.

And so when you think about the liability perspective, you have the data breach notification

requirements, whether it's GDPR or CCPA or any of the 54 jurisdictions across the U.S. that have notification laws, and how they intersect with other sectoral regulations becomes a very nuanced and jurisdiction-specific exercise.

There is an argument to be made for viewing from the perspective, especially if you're looking at a company that has data moving across borders, looking holistically at all of the rights that are available to individuals under the various regimes, whether it's access, deletion or portability, and looking holistically from a sort of 360-degree view of how to implement the structure and a process for addressing compliance for all of those rights in a way that works seamlessly and reduces friction for consumers.

So that's the way we think about it in terms of from a liability perspective. But, of course, going back to the first part, the verification identification, you know, making sure that that part is particularly strong, hopefully avoids the liability pitfalls in the second instance.

MR. BROWN: Thanks, Erika.

One of my goals of my panel is to really give my great speakers an opportunity to kind of illustrate how these things are coming up in some very

different contexts that they're all kind of working and thinking about. So I'm not going to be overly prescriptive with this next question. What I want to open up to all of you is, how are you thinking about it in the various spaces you're working about reconciling the security and liability concerns, and what solutions are you thinking about or have you seen that work to move forward.

And, Michael, maybe you could start off and talk about this in the energy space.

MR. MURRAY: Sure. So I tend to think of security as being downstream from liability. I'm a former, you know, start-up entrepreneur; ran a software company doing energy management. And the security problems are really solvable in my sector. Information needs to get securely from A to B, and that's really not that difficult. Totally, totally solvable, did that a long time ago.

But the liability really, really matters. So the electric utilities typically do not have specific requirements, technical requirements, around security that they have to meet for handling customer data. You know, there's a broad range of, you know, legal regimes and liability that they have, and that sort of drives -- you know, drives the particular

security measures that they take. And one of the models that I think has worked really successfully that I wanted to mention is California. So long before CCPA in 2011, the California Public Utilities Commission adopted some really excellent privacy rules which gave customers the right to share their data with anyone, but most importantly the rules immunized the utilities from a third party's privacy breach.

And this was absolutely critical. So if a customer wants to share their data with Acme Energy, let's say, and Acme Energy, after the transfer has already happened securely, has a subsequent breach, then the utility has no liability for that Acme Energy's behavior. And that was really important because no one wanted the electric utilities to be the enforcer, to be the market policemen. The utilities didn't want that, the energy management companies didn't want that, and so, you know, that's where we -- you know, the liability shifted to one of -- you know, it's whoever causes the harm is the one who is responsible for it. And I think that's just a framework that makes a lot sense and one that we've been advocating for in other states.

MR. CYPHERS: If I can jump in as well -- sorry, Julian. Yeah, yeah, I want to just sort of

"plus one" a lot of what Michael was saying. I think in some context it definitely does make sense for there to be liability for when a company shares data with another company and the other company does something bad with the data; for example Facebook, in Cambridge Analytica. But I think in a lot of those contexts, the reason that the company that does the sharing should be liable is because they did the sharing in a way that was not in the user's best interest and without the user's complete consent or knowledge of what was going on.

But in a portability context, the company that does the bad thing, whether it's accidentally releasing data to the public through like a database breach or something, or exploiting it in a way that users don't like, the person who does the bad thing should be liable.

So another point on security is I think when we start thinking about putting this kind of thing into law or regulation and, like, say, creating a new portability mandate and attaching some sort of security guidelines to it or something like that, one thing we want to be wary of is overspecifying the way security should work in law, because security is a moving target. There is no such thing as a right set

of security practices for the world for even a particular industry, and definitely not over time. Like, things are always changing. And I think in this case companies are -- the companies who are actually working with data and working with users are usually best positioned to make judgments about what kinds of security their customers need. Obviously they have to have the right goals in mind, like companies are not just going to build really robust security infrastructure if they don't have to and if there's no incentive for them to.

But I think if the incentives are aligned properly and companies who do mishandle user data are going to be liable in the right kinds of ways, then the government shouldn't get overinvolved and say, like, oh, you have to use like AES 256 and you have to use this kind of encryption and you have to, like, do this exact series of events to authenticate users. Because I think a lot of times that ends up being counter-intuitive and it can actually freeze in place security practices that might sound reasonable at the time something is written but are out of date a year or two years, and definitely five or ten years later.

MR. RANGER: I'd probably like to "plus one" what Erika, Michael and Bennett have all said for

various different reasons, but I want to go a bit further. So clearly the originator, when you're doing data portability, is responsible for the authentication security, et cetera, as Erika said.

Clearly, as Michael said, when a company gives the data back to an individual, an individual says give it to the other company, the originating company can't then be responsible for use. The individual has taken that responsibility but through explicit and informed consent.

But the look at the security. And what I want to make as a really strong point is -- and I would almost finish with it, but I'll start with it, It isn't a show stopper to data portability and can be fully managed, and we've proven that -- and we're just one company. Lots of companies have done it.

So at digi.me, we don't see, touch or hold individual's data at all. It goes to the individual, decentralized to the individual, which of course greatly reduces the security threat itself. All data is encrypted to a very high standard, and only the individual has the key.

There's a lot more we have to do with data at rest and it being passed around. But we've been audited by governments -- UK, Dutch, Iceland and

various others. We had a wonderful study run by a company called Control Shift in the UK last year with five blue chip companies and the UK government looking at all of data portability and everything else. And they came to one stunningly simple conclusion: It can be made secure and safe. And they looked at us and they audited through everything else.

The EU, though, is saying, you know what, when you've got a company like digi.me or a data intermediary, the individual has to trust them. So they are looking at whether or not there should be appropriate certification of companies that are acting as a data intermediary because we're helping handle all of this data. And I support that. But as Bennett said, don't say exactly how to do it. Do it like ISO 27001 does for security. Just state the principles and the company is audited to the principles. And that works across everything.

So, yes, security is an issue, but it's only an issue because it's an issue whenever you're dealing with data and it's totally, totally solvable and not difficult as a concept. Obviously, you want to be careful how you implement it.

MS. COLLINS: So just to sort of put a button on this, I completely agree with Bennett and

Julian and Michael. I think actually everyone has said this, that security is a bit of a moving target and has to be. Therefore, enshrining it in the law, especially the way the American legal system works, it's a really bad idea.

But I think this makes a very good argument for a technical regulatory that either can put out guidance or something like NIST, which can update companies on the latest security standards. Because I think having, again, an outside arbiter that can say, like, bare minimum, especially depending on your regulatory sector, what data you have -- house, finances, education data, et cetera, is super important.

And while I'm sure companies could come up with a solution among themselves about what sort of data and security standards we'd want them to use, having a sort of trusted outside party, a governmental regulator, do at least some of that work or verify some of that work can really improve trust in a system.

MS. BROWN LEE: So can I just make another point there? I mean, it sort of underscores what we've been saying, but companies can innovate with respect to security, as well. I mean, I think, you

know, you always think of it in terms of products and what not. But I think however it's -- you know, however we approach this, the incentives need to be there to encourage that because I think that, you know, there are ways in which companies can really develop and be on the cutting edge of innovative security, you know, practices. And so we want to make sure that that's not, you know, stifled in any way. I just really want to just underscore that.

MR. BROWN: Thank you, thank you all. Before we switch topics, on the last panel some of you may have heard Peter Swire talk about one of the issues coming out of security of this -- of it being pretextual. I mean, I know we've talked about this a little bit already and in the privacy context, but I wanted to get your sense, at least Michael and Sara, I know you guys have thoughts on this, on how we might be thinking about distinguishing between those legitimate security concerns and those that might be just a pretextual barrier. Are there things we can look to to try to differentiate that or other solutions?

Maybe, Sara, do you want to start?

MS. COLLINS: Sure. I mean, so I think Peter sort of hit it right on the money. If within a

preferred network or within a selection of companies that the data holder might prefer, there's incredibly easy transfer and the security standards aren't as high as the standards they put for outside third-party sharing. That's a really big red flag.

I think another thing that could be a big red flag in the security context is not making it clear to competitors or to data users who would want to do this, what set of security standards you're operating on, like whether you follow, like, a sort of -- a set of NIST security standards, like what your best practices are, so that they can be met.

If it's a moving target or it's really hard to comprehend, or if it's not clear or maybe it changes depending on who's talking to you, that's a pretty good indication that it's probably pretextual.

MR. BROWN: Michael?

MR. MURRAY: Yeah, I think Professor Swire had a great point. This sort of differential requirement comes up with utilities quite a bit; for example, with authentication requirements. So if the utility is trying to authenticate you so that you can pay your bill, your monthly utility bill on time, they make that extremely easy and there's a very minimal set of authentication requirements, your account

number, maybe your telephone number and that's it. But then when you want to share your data with another entity, they throw the book at you. And there's -- you know, you need to know, oh, what was it, it's like my cat's maiden name or something like that. There's all these pieces of information that you need to require. And that's just a very simple -- you can just look at those two requirements and say if they don't match, well, then it's probably -- there's some anticompetitive impulse here that needs to be, you know, squelched.

And the second thing is, just to tell a brief story, I asked a utility last week to -- they had proposed a data-sharing system for third parties with permission; it sounded great. And I said, well, tell me what are your requirements for these third-party recipients. And they said -- you know, they gave me some standard forms, which was expected. And then they said, you also have to agree to company cybersecurity policies. And I said, okay, well, give me a copy of those cybersecurity policies because my members have to meet those requirements.

And this is when the utility, who will remain nameless, said, sorry, that's all confidential. And so, in my experience, these cybersecurity concerns

are -- it's really about wielding power and control. It's not really about your security requirements. If you have to hide your security requirements, they're probably not legitimate. We know that security through obscurity doesn't work.

MR. BROWN: Thank you, both. I'm hopefully not cutting anybody off, but I'd like to move now to another kind of intermediate topic that really I think elides security as well as standardization -- and I'm going to ask Bennett maybe to discuss this at first. And that's the issue of credential sharing, or as other panelists today have called screen scraping.

Bennett, could you explain a little bit, what is this idea of screen scraping and how does it fit into the subject of data portability in your mind?

MR. CYPHERS: Sure, yeah. So screen scraping in general is this practice of one company or anyone, really, running, like, a headless browser or a piece of technology that's instrumented to look like a regular human user interacting with a website or with an app. But that actually is automated and can scrape or collect data from an interface that is designed to be interacted with by humans.

So this is, like -- this comes up in a lot of different contexts, but with portability, it

usually means, like, something like Plaid or Mint, where you have an account with, say, a bank or a different kind of institution and you want to access the data -- you have some data in that institution that you can access through, like, some sort of web interface, but you want to grant access to it to another company who can, like, do some cool analysis, or reformatting of that data on your behalf.

And so what you do is you might grant -- you might give your credentials to an intermediary. That intermediary will take your credentials and log into the bank or other company on your behalf, and, like, use a headless browser to read the data from a human-readable webpage into a computer, and then do whatever they want with that data, or hopefully whatever the user wants.

So this is -- this is a practice that is part of a broader sort of set of practices that we like to call a competitive compatibility. And this is where, like, one company or organization has information that a user might like to use in a way that the company doesn't allow or doesn't support. And other companies can step in and say, like, hey, you know, your bank's not going to do this thing for you, but we can do it on your behalf. And so we're

going to -- even though the bank doesn't offer, like, APIs or technology to do this specific thing, another company can work around -- work with what the bank does offer, which is often a webpage or an app, and find ways to use that information in new and creative ways for new and creative products that users might like.

And so screen scraping is sort of one technique that's often used for competitive compatibility purposes. Obviously, it can be used for nefarious purpose as well, and this goes back to, like, the need for comprehensive privacy law to make sure that when you do grant your credentials to someone and say, like, hey, like I want to see a cool spreadsheet with all my data in it, they're not going to turn around and, like, use your password for other stuff or sell your data to someone else without your knowledge or consent. I hope that's a decent introduction.

MR. BROWN: Thank you. I'd like to give other folks -- and, Bennett, you can add to it as well if you have more to share -- just a quick chance to talk about how does this play a role in data portability. Is it effective? Can it be a way to not have to deal with the problem of standards? You know,

what do you guys think of it? Maybe Michael -- sorry, Julian, did you want to start?

MR. RANGER: Yeah, I was just going to jump in if you don’t mind. I don't think it replaces standards or whatever. Look, if asked the question, are APIs a better alternative than screen scraping for data portability, the answer is yes, a thousand times yes. Right?

Screen scraping is the last possible thing that you want to do. You're giving your credentials to a third party, and that may be abused. It may open up liability to the data originator because nobody's approved it. It's no good. But -- and here's the point: It has to be legitimate if the data source company isn't providing my data back to me in any other form. Right?

So if you had a law that was absolutely explicit that you had to have data portability via APIs, which is our recommendation, then you could ban screen scraping, and I think that would be a good thing. But in the absence -- if I can only get my data back or allow it to be used in another service through screen scraping, then, I'm sorry, that's what I have to be able to do.

So it is not the right answer, but it's an

adequate answer in the absence of data portability via APIs. And that's the key thing to say.

MR. BROWN: Erika, did you want to add something?

MS. BROWN LEE: Yes, yes. Thanks, Jarad. Just a quick addition, because it is a topic, obviously, that is, you know, very important in the financial services sector. And, you know, not everyone in the industry participates, but I wanted to sort of mention that there is work being done in the industry by the financial data exchange, or FDX, which, you know, is working to coalesce around common interoperable standards for the -- for an API, an FDS API, for consumers and businesses to access their financial data.

So, as Julian mentioned, when you have an API, you're not sharing the credentials like passwords and user names. That stays with the individual themselves. And the individual themselves gets to choose, you know, who and how their data is served, you know, or is ported or used.

So you have the advantage of API standards that would give consumers additional transparency, additional control, and it also addresses that security piece as we were just talking about, where,

you know, you worry about how it's being used onwards or by the intermediaries who get the data.

This, of course, if you don't -- or if you're not sharing the credentials or the passwords in the first place, it takes away a level of security threat risk. And so in light of those benefits, certainly there is -- you know, it's important to sort of think through and support standards that are developing within the industry. So we see that in the financial services sector, and that might be, you know, an example for other sectors as well.

MR. MURRAY: You were just on mute, Jarad, but I'll jump in. So screen scraping is really not ideal. A lot of companies use it in the energy sector. We don't want to. Nobody likes to do it, right? It's expensive. It can be buggy. It can be inconsistent. Utilities change their website; we have to accommodate it. It's just a silly cat-and-mouse game.

But the reason why it continues is, one, there isn't a good alternative, APIs. But I think there's a couple of other things that play at least in the utility industry. I think the utilities like having -- like screen scraping being sort of the only option because, you know, then they can, you know,

claim, you know, CFAA violations and get legal on these incumbents who are trying to access this information with customer consent. It's sort of -- it's just a convenient way of, you know, running out the clock and, you know, incurring a lot of costs for those entities.

But I think there's another case that we also have to be careful of, which is where utilities can also manipulate screen scraping, too. So it's not that screen scraping is the best, always true source. There have been cases in the financial services where banks have, you know, started withdrawing information from their web portals because they didn't want that to be scraped and available to competitors.

And, similarly, we've seen a couple instances where utilities will say, oh, well, you know, we're only going to put your bills online if you agree to, you know, have ACH payments for your monthly utility bills. And so there's this, like, sort of withholding of information that can happen both in the API sector as well as getting data through screen scraping on these incumbents' websites.

MR. CYPHERS: Yeah, and so I could just make another couple of points. Screen scraping, as everyone has said, is never the best option. Like,

obviously, if there's some kind of data that you would like to port or use for a secondary purpose, it's always better, for everyone involved, if there is an API for that specific piece of data.

But where screen scraping comes in is when the data holder doesn't want to share that data, or they're not compelled to, or there's a law that says they should be sharing this data but they can find a way to interpret that law that says, oh, we don't actually have to share it in this form, or we don't actually have to share the critical piece of it that people need to make it useful.

And so screen scraping, I think our perspective is to disagree a little with Julian. Screen scraping should never be banned. There should never be a law that says that you cannot scrape a company's screens for this kind of data. You can talk about bans on specific uses of screen scraping, which is fine. But, I mean, EFF's position in general is that CFAA is an overbroad law that can be used to shut down a lot of very legitimate activities, screen scraping in a competitive compatibility context being one of them.

And the other reason it's important is because it -- like, regulations are really hard, new

regulations are really hard to create. And the tech sector, especially, is moving really fast, and there's going to be new kinds of data and new industries where people want to use their data for new things, and regulation is never going to be able to keep up with that no matter how much we might like to believe that it is. And so there's always going to be, like, things that people want to do with their data where there is not an API yet or it's not in a company's interest to make an API for that particular data, and regulators can't catch up fast enough to say, like, you have to make an API for this. And so keeping screen scraping as sort of a last-resort option that competitors can always fall back on we think is invaluable and actually necessarily.

And screen scraping as an option actually makes it beneficial, like, for data holders to create APIs a lot of time. And, like, we saw this in the financial services industry 10, 15 years ago, where, like, Plaid and Yodlee and Mint were scraping data from banks, and banks didn't like that a lot. But they realized that customers really liked the product that those aggregators were putting out. And so eventually that helped pressure them into creating these APIs that a lot of banks now do support, and

it's better for everyone, especially consumers.

MR. BROWN: Thanks, Bennett.

I'd like to shift us now to the last subject we want to talk about today, which is a critical one, and I apologize as a privacy and security lawyer for at all giving this short shrift. But we want to talk about standardization and interoperability and get your great thoughts on that.

All day we've heard speakers talk about how important these two aspects are to helping realize many of the benefits of data portability.

I want to start off with Julian. It's been a while since Peter Swire's presentation this morning, and I thought maybe you could talk a little bit about what are we talking about with the difference between these two concepts and their goals, and then how do you think they fit into data portability initiatives?

MR. RANGER: Okay. So I'm going to be a bit controversial here, because I believe totally in interoperability but want to see standardization delayed so that we get on with data portability and bring standardization downstream. Interoperability is different. Interoperability is the ability to effectively exchange data, not perfectly, but effectively. Standards help with that. But I can

create interoperability where there is no standardization, right, as a business.

We do that at digi.me. We normalize all data received by the individual no matter what data format it arrives in, all to a single normalized ontology, and that creates interoperability as any system using the data gets the data in a single form no matter what the input.

So if you use digi.me for health data, it doesn't matter whether it's U.S., UK, Dutch or Icelandic, you get it one form. No standards required. I can assure you that there's umpteen different implementations across that set, even though nominally most of them are following a standard called FHIR, but even then it wouldn't work. So you must distinguish between interoperability and standardization.

Now, standardization makes interoperability easier, so if more parties use the same standards and are really compliant to those standards -- that's the real key -- then my job at digi.me is made much easier, as is everyone's. But their standards are not a panacea. There are always interoperability issues even with standards. And I spent 20-plus years doing this for the military. I was called "Mr.

Interoperability." I made a large amount of money solving the problems. And standards help, but they don't solve all the problems.

So it's for that reason that I strongly -- and I sort of say that strongly times 100 -- that the EU -- like the EU has done, data portability comes first, specifying something along the lines of a well-formed API but without specifying the standards. Get the data moving first, and then let businesses solve the interoperability problem, then get the standards developed and implemented for each sectoral area. But please, please, don't wait for standards before opening up the data or you'll never get to the new data economy you want.

And as a final cautionary tale, look at the -- and I'm sorry to do this to you, my colleagues and friends in Australia because we work there, but the Australians have the consumer data right, and it's adopted a standards-first approach to opening up the data, and it's frankly a mess. Right? It is a mess. It's heavily delayed, much to their economic detriment, across the whole thing. All right?

So in this case, follow the EU. Open up the data, well-formed API, any format, businesses will solve interoperability. But then really encourage --

and standards because we all want them, but let it follow opening up the data.

MR. BROWN: Thanks, Julian.

And I think -- my other panelists, I suspect, will have some interesting thoughts to respond to your suggestions. But I want to first turn to Michael to talk a little bit about your experience with standards in terms of how those have played out in the energy sector as an interesting case study, and what you're thinking and recommending for the future based off what's happened so far.

MR. MURRAY: So the standards and energy came, actually, out of the American Recovery and Reinvestment Act originally. There was some great work done by the FCC in the National Broadband Plan, which I hope folks are brushing that document off as a potential guideline for economic revitalization post-pandemic.

And one of the key principles, one of the key objectives, in the National Broadband Plan at the time was for every American to have access and the ability to share their real-time energy usage, using home broadband connections. That's from 2010.

And so that's sort of, again, a standards development process led by NIST, the Department of

Energy, Smart Grid Interoperability Panel, and others, and it resulted in the standard we now call Green Button. And it's -- you know, it's been used, the Green Button has been adopted as the API version of it, in about five states covering 36 million electric meters. There's about, you know, 120 million homes across the U.S. So, you know, it's a sizable percentage of the total.

And the standard was -- it was, yes, there was some important things technically to be done there, but to be honest, it was mostly politically important because it was -- the lack of a standard and the lack of federal involvement, you know, pre-2011 in this area was just a really great reason for the utilities to say, oh, you know, nobody can even agree on a standard, so let's not do anything; let's just, you know, pretend this whole issue disappeared.

And so I think that sort of political leadership helped make it possible, that there was, you know, buy-in from the government and industry and a lot of players.

Now, with that said, I think Julian is exactly right. Standard is just one tool in the toolbox. Just because, you know, two entities claim to follow the same standard doesn't mean you have true

interoperability. And one of the challenges that I think we have in energy that maybe you don't have in a sector like banking is that the banks have a bit of an incentive for interoperability, because although they might not like their information going to their competitors, they want to be able to get their customers' information that's held at their competitive financial institutions.

And so there's a bit of a backflow in terms of data that can benefit them. And utilities just don't have that incentive whatsoever. If I move from Baltimore to Florida, the Florida utility really doesn't gain any value whatsoever on my usage history in Baltimore, and so -- and that's why it's much easier for, I think, utilities to just sort of, you know, dig their heels in and say, you know, we're just going to do the bare minimum, provide the absolute bare minimum of data and maybe not even fully comply with the standard. And that's why I think there's a much bigger need for not necessarily standards development but standards enforcement.

MR. BROWN: Thanks, Michael.

I'd like to open it up now to my other panelists to respond to what you guys have both said in terms of examples and also maybe just address what

models you think work for getting us to standardization or interoperability and what should be first. And maybe, Sara, could you go first?

MS. COLLINS: Yeah. So, again, we are big proponents of interoperability. And while I appreciate what Julian said, I do think things happen, like what Michael's described, when there isn't a business interest to incentivize interoperability. You can imagine there's a large dominant social network which has all of the people on it. There is an up-and-coming social network that you or myself would like to try. However, no one else is on it. So you spend a couple of hours there, get nothing out of it and then go back. You may have even moved all of your data, too, so all of your photos and other things are there, but nobody else is there, either.

The large dominant platform has no incentive to create an interoperable system where you can post or interact between those two because it doesn't benefit them. So while I don't think there's anything wrong with sort of these organic systems coming up naturally, I do think where there's significant competitive concerns you have to get a mandate from either the legislature or a regulator, and you may have to do the really nitty-gritty standards process

to get it to move in order for it to be useful.

MR. CYPHERS: Yeah, I'd like to just give a huge “plus one” to what Sara just said. This is a portability panel, and we’ve talked a lot about portability. But to solve, I think, a lot of the bigger issues that we're looking at in the tech sector right now, especially around competition, portability is good but it's just not enough. It’s not enough to be able to take your data, take, like, the names of all of your friends and move over to Martagon because none of your friends are going to be on it and Facebook -- sorry -- and the large incumbent social network has zero incentive to, like, allow you to interact with people off of its platform who don't have an account with the large incumbent social network.

And so it's about -- like, portability gives you this outflow of data. It lets people take their data and take it somewhere else, but you -- to have real competition and to undermine the network effects that can be so powerful in a lot of these sectors, you need the inflow. You need the other direction where the company has to say, like, yes, we will respect people who don't have accounts on our platform as real people and allow them to interact with our users on a

level playing field.

And I don't think it makes sense -- I don't want to get overbroad here and say, like, oh, every company that exists should have to do interoperability using these standards, but, like, when you have these giant, pseudomonopolist platforms that just control everything and it doesn't look like they're going anywhere anytime soon, I think those deserve special regulation to say, like, hey, you know, you have to play with these other up-and-coming platforms on a level playing field; you can't just have all your users and let inertia carry you forward forever.

MR. RANGER: Well, I suppose, Sara and Bennett, whilst I agree with you, that isn't data portability. That's a more broader competition point. And so I'm not going to disagree with you on the competition point at all.

But on the data portability point it would be dangerous, and that’s why I’m saying. Because it would delay the availability of data, and that's the worst possible thing that could happen to us all.

MR. BROWN: Thank you, all.

Oh, Erika, I was actually just going to turn to you and just ask you a little bit from the business perspective, your thoughts on what your co-panelists

have said. So, please, take it away.

MS. BROWN LEE: Sure, sure. I think, you know, we're all in agreement in the sense that, you know, there's support broadly for interoperability as an overarching principle and standards in particular.

You know, just sort of adding onto some of the comments, I would just suggest that industry participate -- that industry participation in development of the standards is also important because if you -- without it, ideally you want to be able to have and build scale and adoption. And, you know, if standards are set in a particular rigid fashion where there's asymmetric adoption, that also can have, you know, a negative impact on consumers, in particular, because they won't be able to -- you know, there will just be some players that don’t participate.

And so, you know, I think that point of having a level playing field is important, but I do think that, you know, there does need to be sort of industry participation and recognition of not only the various differences within an industry, but also between industries.

MR. BROWN: Thanks, Erika. And thank you all for jumping in on this.

We have just a few minutes left, and I'm

going to move to give my panelists an opportunity to just throw in some closing thoughts if they want to sneak in any responses to what we've just said. I'll give them that chance there.

And, Erika, I'll switch you to the end of the order because you just spoke, but maybe, Sara, could you go first, and just give us a minute or so of any closing thoughts you'd like?

MS. COLLINS: Yeah, I think data portability really shows how interconnected some of these very hard questions in this sort of digital economy are, and that if we're going to -- that we can't think about data portability as if acting by itself. It affects privacy. It affects security. It obviously has implications for competition.

So while obviously creating rules around data portability you need to have a focus, I think there also needs to be a sort of perspective of looking around at how it will affect the larger digital ecosystem going forward and what exactly we want out of that ecosystem.

Obviously at Public Knowledge, we want it to be user centric and user friendly and ultimately not harmful.

MR. BROWN: Bennett, would you like to go

next?

MR. CYPHERS: Sure. Yeah, I'll try and make a few points very quickly. First, mandates are great, where we can get regulators and users and industry to agree on what the right data is to be sharing, and what the right APIs look like. But competitive compatibility is key to allowing small upstarts and tinkerers to innovate on data portability and figure out what kinds of uses for their data there might exist if companies are not moving forward with APIs and regulators can't keep up with new technology.

Finally, we need a privacy law. We need good privacy law in the United States. We don't need it as a prerequisite for data portability. Data portability doesn't create new risks to privacy, but it should bring attention to the risks that are already out there and remind everyone that data is not always going to be used in your interest if there are not liabilities and incentives for companies to use data in ways that you would like.

MR. BROWN: Michael?

MR. MURRAY: So I'd like to end with a request. Given this large patchwork of utility regulation, including state, public utility commissions, city councils and cooperative boards, all

of them are struggling with what the heck is informed consent. And so if I had a request, it would be to the FTC, and I would -- I would, you know, humbly, respectfully, on one knee, ask that the federal government and the FTC please provide some guidance on online consents and what they should look like and how they should function.

The Consumer Data Right in Australia, they've done some fantastic work through CSIRO, that's their NIST equivalent down there, and it's just amazing to see, you know, actual screenshots of, this is what it should look like. And that's exactly the level of detail that we'd love to see, because there are tons and tons, you know, thousands of regulators who oversee electric utilities who are all scratching their heads saying, we don't know what informed consent is.

MR. BROWN: Julian. You're on mute, Julian.

MR. RANGER: I'm going to add to that previous question by saying, of course, look at the digi.me consent certificate because it hopefully is best practice. But, plus-one to what you've all said. I think the key point is that with data portability, access to data is no longer going to be the competitive barrier it is. And that's the

point.

Any company can get better data than the big four or five have today if the individual consents. And it's the value that you offer individuals that causes them to agree to share their data that becomes the determining competitive practice. So if I can misquote your own declaration, all companies then become equal when it comes to data. So data portability is an absolute key. It doesn't solve the other competitive issues, but it solves the data competitive issues.

MR. BROWN: Thanks.

And, Erika, I'll give you the last word.

MS. BROWN LEE: Well, I know we're over, so I don't want to take too much of it. You know, I think everyone has really expressed a lot of what I would say. Certainly as individuals become increasingly aware of the uses of their data, they're demanding more control, and so portability is an accord of that. And to the extent that we can -- as we see these proposals coming up across, you know, the various jurisdictions, you know, and hopefully drive, you know, concerns for interoperability as a consistent approach, I think we would all benefit. So I'll just sort of end my comments there.

MR. BROWN: Thank you all for a really great discussion this afternoon. Thank you for all your time and contributions in this process. And thank you, viewers, for joining us.

I'm now going to hand it over to the Director of the Bureau of Competition, Ian Conner, for some closing remarks. Thanks.

(Brief pause.)

CLOSING REMARKS

MR. CONNER: So thank you all for joining us today and for participating in today's timely, excellent discussion. This was a great event with a great lineup of speakers. And while I wasn't able to attend every session, I am pleased with how the day did unfold.

Data portability is one of those issues that cuts across the FTC's work. It raises questions about how best to protect consumers and promote competition.

As a law enforcement agency, the FTC carries out its dual missions primarily by using its law enforcement tools. We find and stop conduct that directly harms consumers or denies them the benefits of competition. But just as important as finding and stopping those law violations is how we fix them. Our remedies must address the sources of harm. This is always a challenging exercise, but it may -- it can be particularly challenging in the digital sectors, especially data-driven ones.

More and more, businesses are relying on a steady stream of data to serve customers, develop new products, and improve operational efficiencies. Acquisitions can involve the acquisition of data itself or raise concerns because of the ability to

harvest more data or foreclose data access to rivals. Whether data is available and can be moved is a key issue in understanding the competitive implications of both acquisitions and conduct by market participants.

Today's discussion highlighted some of the challenges of understanding how data is used and moved, and, more importantly, how those practices might affect consumers and competition. Because data will continue to be important to consumers and competition, understanding what is at stake is of critical importance to the Federal Trade Commission, and we are grateful to our panelists today that you have given us so much to consider. Your hard work was evident and you have provided us must intellectual food for thought, so I thank you.

Data's a competitive role and its portability is not just a question assessed in looking at the effects of a proposed transaction or practice. It is key to understanding what it is going to take to remedy potential or actual competitive harms from those transactions and that conduct. Without understanding the role of data portability, we can't fully assess the remedy necessary to address those competitive harms. And making more and more users' data more accessible and held by more entities can

itself actually raise privacy and consumer protection concerns that we must consider in crafting our competition remedies.

Our panelists have given us a lot to consider on these issues, both from a competition and from a consumer protection standpoint. In addition to the informative and thoughtful presentations from our panelists today, I would also like to thank the groups of individuals who have filed comments in response to our initial workshop notice.

I would like to close by acknowledging our organizers for their enthusiasm, dedication and patience in assembling today's program, especially under such challenged circumstances as have been brought on by the pandemic. It takes many people to organize workshops such as this one, and our team included staff was from all three bureaus and our Office of International Affairs.

Thus, although it is late in the day, please indulge in some well-deserved expressions of appreciation from myself in the Office of Policy Planning, the Bureau of Competition, the Bureau of Economics and the Bureau of Consumer Protection.

For our planning team, Andrea Zach, Jarad Brown, Chris Grengs, Ryan Quillian, Guilherme Roschke,

Kelly Signs, Leah Singleton, Ben Smith, and Kate White.

For our workshop and logo work, Daniele Apanaviciute; from our Office of Public Affairs, Juliana Henderson and Nicole Drayton; for today's webcasting, Bruce Jennings and our Web Team; and last but definitely not least, our events planner, Kristal Peters.

It is our staff members who make workshops like this one possible and productive, and it is our staff who work tirelessly every day to investigate, and when necessary, go to court to protect the American consumers. Thank you very much for your attendance. Have a good day.

(Hearing concluded at 2:57 p.m.)