Privacy Roundtable: Recent Developments and New Frontiers

MODERATORS

Aaron Burstein *is a partner in the Privacy and Advertising practice at Kelley Drye & Warren, and an Associate Editor of* Antitrust *magazine. He advises clients on compliance with a broad range of privacy, data security, and consumer protection regulations, helps businesses build privacy programs, and represents clients in enforcement and oversight investigations.*

Janis Kestenbaum *is a partner in the Privacy and Security practice at Perkins Coie LLP, and an Associate Editor of* Antitrust *magazine. She represents businesses in privacy and consumer protection investigations of the FTC, State Attorneys General, and foreign data protection authorities, counsels on compliance with privacy laws, and advises on the development of privacy legislation.*

PARTICIPANTS

Will DeVries *is Senior Privacy Counsel for Google, advising Google on global data protection compliance and product development. Prior to Google, he taught Information Privacy Law at the George Washington University Law School and worked in the Communications, Privacy and Information Law group at WilmerHale LLP.*

Alexandra Reeve Givens *is CEO of the Center for Democracy & Technology, a leading nonprofit organization based in Washington D.C. and Brussels that advocates for technology policy and architecture to protect consumers and civil rights.*

William McGeveran *is the Associate Dean for Academic Affairs and Julius E. Davis Professor of Law at the University of Minnesota Law School. His teaching and research has focused on data privacy law for over 15 years. He is the author of a casebook,* Privacy and Data Protection Law, *which is used in many law schools.*

Jessica Rich *is a Distinguished Fellow at the Institute for Technology Law and Policy, Georgetown Law. She served as Director of the FTC's Bureau of Consumer Protection from 2013 to 2017, capping a 26-year career leading the agency's enforcement and policy efforts related to privacy, security, technology, and financial fraud.*

Editors' Note: *On October 2, 2020, a group of leading privacy lawyers from civil society, the technology industry, and academia spoke with Aaron Burstein and Janis Kestenbaum, Associate Editors of* Antitrust *magazine, for a roundtable conversation. The wide-ranging discussion covered legislative developments in privacy at the state and federal levels, privacy issues that emerged from both the COVID-19 pandemic and recent protests for racial justice, privacy developments in the European Union and their impact on American businesses, the interplay between privacy and competition, and what the FTC is and should be doing in the privacy arena.*

JANIS KESTENBAUM: We are having this conversation about a month before the November 2020 election, so we would like to start by talking about California, where privacy is on the ballot. On November 3, California residents will vote yes or no on the California Privacy Rights Act (CPRA), also known as Proposition 24. This ballot initiative would substantially amend or expand upon the California Consumer Privacy Act (CCPA).*

It was just two years ago that the California Legislature adopted the CCPA, which was heralded as the broadest consumer privacy law in the United States, and frequently compared to the European Union's General Data Protection Regulation (GDPR). The CCPA only went into effect in January of this year, and became enforceable by the California Attorney General in July of 2020.

My question for Bill is: Why are we seeing an effort by the architect of the CCPA, Alastair Mactaggart, to overhaul his own handiwork so quickly via the CPRA ballot initiative? What is Mr. Mactaggart seeking to accomplish?

WILLIAM McGEVERAN: I think Mr. Mactaggart—and it's not just him; it's a team of people who he has recruited

*The CPRA was approved by California voters on November 3, 2020.

into his efforts—their perspective is that, although the law passed, they characterize what has happened since that time, with the Attorney General's regulations and some efforts to amend it in the Legislature, as being efforts to water down the original bill. On that basis, they have come around to the view that privacy rules should be spelled out in the California state constitution rather than contained in a statute that is more subject to change.

So while Proposition 24 would make a grab bag of substantive changes, you ask what is motivating the proponents, and I think it is as much about process as about content. They want these rules to be enshrined in the state constitution and they want to have a separate privacy commission in California, like European countries do. That, I think, is driving them more than some of the individual provisions, which are also significant—things like increasing fines for violations involving children and adding provisions about geolocation and sensitive information—but probably the driving force is this idea that they do not trust the political process to be the venue where privacy law gets resolved.

JANIS KESTENBAUM: The CPRA is reportedly polling very favorably with voters, but it has splintered consumer and privacy groups. Some vocally support it, like Consumer Watchdog; some have openly opposed it, like the American Civil Liberties Union; and others are neutral, like the Electronic Frontier Foundation.

Alex, a few related questions for you. First, has the Center for Democracy and Technology (CDT) taken a position on Proposition 24? Second, why we are seeing this divergence of views among civil society, and can you help us understand what the concerns are of the groups that are opposing Proposition 24?

ALEXANDRA GIVENS: CDT has not taken a position in this fight, although we are obviously following the conversation very closely.

The CPRA makes a couple of really notable improvements that we do value over existing law. Some of those—just a laundry list: there is an important fix to regulate the sharing, not just the sale, of data; it adds protections for the use of sensitive data, with a broad definition of "sensitive data" that we think shows important movement and is something we are trying to push regulators across the country to understand; and there are some data minimization principles in there that are important, although we do have some concerns about how those are drafted.

The core areas of controversy that are driving a lot of this debate: one is this notion that the CPRA potentially enshrines or reinforces the concept of "pay for privacy." Companies can charge more for privacy protection and provide inferior services to people who opt out of data sharing. There is a real concern that this will penalize people who opt out of sharing their data, which could deepen the privacy divide between low-income and high-income communities. I will say that there is language in there that any of those payments have to be proportionate to the value of the data, for example, and there is some disagreement over exactly how much the CPRA is changing because in some ways this notion is already present in the CCPA. But, regardless, any movement that is further in this direction is very troubling for consumer advocates.

There continues to be a lot of disappointment that there is no private right of action in there.

And then for CDT, one of the reasons why we continue to have mixed feelings about the efforts in California is that really at bottom it still underscores "opt-out" as the mechanism for protecting consumer rights. It has clear language about the nature of the notices that can be required, but, as a general principle, when we think about ways of protecting consumer privacy, relying on opt-out simply has a lot of flaws.

There is a report that came out from Consumer Reports this week analyzing people's behavior in California that gives some empirical evidence for the insufficiency of opt-out. That is something that CDT has been focused on for a long time, and really does think the conversation has to move beyond.

JANIS KESTENBAUM: California is not, of course, the only state that has been focused on privacy recently. We have seen a lot of activity in other state legislatures as well. Bill, can you bring us up to speed on what is happening in other state capitals with regard to privacy? How has COVID-19 affected the momentum of efforts to enact new state privacy laws?

WILLIAM McGEVERAN: Most state legislatures are now out of session for the year, but this year we saw a huge number of proposals introduced in state legislatures, much more than had been the case in the past, and there is already a lot of discussion about bills in 2021. I think that the action in California has really catalyzed that in a significant way.

I actually have a law review article coming out soon that I co-wrote with Anupam Chander at Georgetown and Margot Kaminski at Colorado discussing this phenomenon, that now that the CCPA requires companies to take certain kinds of actions, it is stimulating interest in other states in two ways: (1) They are saying, "Well, privacy law is now becoming more serious in California and so maybe we should have more robust privacy law here in our state too"; and (2) from both state legislators and companies an interest in saying, "Well, what we don't want necessarily is to have all of these obligations in California and then have some inconsistent sets of obligations in other states." So states are looking for how to address the patchwork.

We saw a bill almost pass for two years in a row in Washington State—I think it's still possible that that bill might eventually come through—and lots of committee action in many states. A bunch of states ended up enacting

commissions to explore this, which sometimes is a way of filing something away forever but could also be an impetus, when these commissions' reports come back, for those states to take legislation up. I think in at least Illinois and New York, arguably Massachusetts, possibly Maryland, and maybe some other states as well, we could see some real movement towards legislation.

Two other quick things. One, there is also the Uniform Law Commission, which is the body that is responsible for the Uniform Commercial Code and lots of other model statutes that get adopted in the same form in multiple states. The Uniform Law Commission is working on a uniform consumer privacy law in response to what happened in California. A lot of states may find that to be a mechanism for having both more robust law in their state but also uniformity, if that effort moves forward successfully.

Second, in response to your question, I think the COVID-19 pandemic has changed the debate in a lot of ways, but I wouldn't necessarily say that it has slowed it in states. One thing that happened is a lot of states became more aware that privacy law is not really well fit for 21st-century challenges, and this public health crisis became another situation where privacy law was not designed to meet the moment.

So, if anything, I think the pandemic might actually spur thinking about what privacy law should look like—of course, accommodating important interests like public health. I don't think it necessarily puts a damper on interest in moving forward with some changes.

JANIS KESTENBAUM: What is the status of the Uniform Law Commission's work to create a model privacy law?

WILLIAM McGEVERAN: They have an open process by which anyone who wants to be an observer can join and give comments, and actually there has been lots of interest. Jessica has participated as an observer, and quite a few advocacy groups and quite a few tech companies have been represented there.

They are still in the committee drafting-and-debating phase, but their target is to have something that the full Uniform Law Commission could approve in 2021. If they meet that goal, then the legislation would be ready to be potentially enacted in individual states as soon as this time next year.

They took the scope of the CCPA as their starting point, but they are drawing on lots of different state efforts, and I think it is still in flux what the exact nature of that bill will be when it comes out the other side of the process next year. But they are moving quickly and they are working hard, so I think that will be yet another input into the debate about what privacy law ought to look like at both the federal and the state level.

AARON BURSTEIN: Let's go back to the point that Bill raised about COVID-19. That is one of two major U.S. and world events with a thread of data use and privacy running through it. The other is the protests surrounding the Black Lives Matter movement.

Starting with the coronavirus, the idea of smartphone-based exposure notifications and contact tracing through smartphones was heralded as a promising way to slow the spread of COVID-19. Now that we are many months into the pandemic, could we ask you, Alex, to give us an assessment of how this idea has played out in practice.

ALEXANDRA GIVENS: CDT mobilized really quickly on this issue. At the beginning of the pandemic, we convened a task force of civil liberties advocates, representatives from industry, and civil rights advocates to talk about the potential tech solutions that might be used and to make sure that people were focused on ways to address and minimize the privacy risks.

Just to give an example, some of the things we were worried about include the use of location data to enforce quarantine, which has happened in some other countries but not in the United States; and with respect to exposure notification apps, a real concern about the potential for disparate impact in how those tools can be used.

What's interesting is that the adoption has not been nearly what we expected. The government has barely been organized enough to encourage people to wear masks. Some states are encouraging the use of these tools—New York and New Jersey rolled out exposure notification tools this week, for example—but so far we have had fewer concerns than expected about the mandatory adoption of those tools.

One thing that we are looking at is whether that changes as more people start going back to work—if employers are starting to think about the mandatory adoption of these tools. If things go in that direction, we do have real concerns because of questions about validity and accuracy and the conditioning of access to the workplace or public accommodations on these tools, as opposed to using the tools simply as a useful aid to guide people's decisions and health choices, as opposed to the yes-or-no that determines whether or not you have access to your workplace.

One last point is that the companies have been really thoughtful in the development of these technologies—for example, in the strict limitations about who can create an exposure notification app to begin with, the requirement that it be authorized by a health authority. I think that has been an important piece of this puzzle, in making sure that the tools are seen as a useful guidepost but have not been perhaps as troubling for civil liberties as we might otherwise have feared.

AARON BURSTEIN: Let's continue with that point. Will, what role has the private sector played in the development of the underlying technologies? And how are companies addressing some of the concerns around privacy and other issues that Alex mentioned?

WILL DEVRIES: At Google, we watched this when it was breaking back in February-March with alarm and a lot of questions about what we could do. We asked how we could leverage the tools and the reach that we've got to provide some benefits to our users and to the communities that are fighting the virus. As Alex indicated, we knew that health agencies would take the lead on this. We didn't want to step into that role, but we obviously have a big role to play in the technology layer.

One response was a project called "Community Mobility Reports." That was a good example of trying to leverage data that we already were using for our consumer services to get some aggregated insights into how mobility patterns would change in response to the pandemic. This can help health agencies, the media, and others to see where people are moving, are they moving more or less, and how they are responding in terms of the restrictions imposed on movement and stay-at-home orders. The analytics there were anonymous, and we employed differential privacy, meaning we add artificial noise to the data sets so that you can get high-quality results and see on a local level what is happening without identifying any individual person.

And then, as Alex mentioned, we formed a partnership with Apple to develop a protocol for exposure notification. Exposure notification is playing a big role in slowing the spread of the virus. The technology that we developed is going to inform people if they have been exposed to someone with a positive diagnosis of COVID-19 by using the technologies already embedded in the smartphones that everyone carries around with them.

We use cryptography and on-device storage so that we can notify users about the exposure without actually collecting or sharing any individual identity with the government agencies, with the platforms themselves, or with other users. Apple and Google require that the technology be opt-in only, so people have to use it voluntarily, and we can technically prevent exposure notification apps from trying to get location or the contact information from the devices. If health agencies want that information, they are going to have to obtain it in different ways.

The privacy design of this is critical. What we realized really quickly is that if it didn't have privacy at the forefront it would never be adopted. People want to be able to trust that this is purely for their health and to respond to this crisis and not something that is going to be misused later, so we clearly wanted to establish and keep that trust.

I believe at this point there are 12 states that have now implemented the contact tracing API, including New York and New Jersey just recently, and a growing list of countries abroad. We hope that that increases very quickly.

We will be turning this down after this COVID-19 crisis is done—this is a limited response—but we hope we can of course learn from it because unfortunately another pandemic could occur in the future.

JESSICA RICH: Could I just interject a couple of big-picture points about COVID-19 and these contact tracing tools? I think, despite efforts by many, there is enormous disappointment in our ability to use these tools to help us deal with COVID-19. I see three lessons, two of which relate to privacy and the discussion we are having.

The first is, of course, when you do not have comprehensive testing—and these tools started rolling out when testing was in a terrible state—these tools have limited utility because they build on the idea that a person has been diagnosed with COVID.

Second—and this is where we get to the privacy issues—consumers haven't wanted to use these tools because they don't trust the companies or agencies deploying them and are wary of allowing them to collect their data. Sure, companies announced voluntary protections, but there were no rules or laws guaranteeing these protections. The Health Insurance Portability and Accountability Act (HIPAA) has some vague language in it, but the law doesn't apply in many instances and the language doesn't mean much.

Third—and Bill touched on this—I think this shows us that having privacy laws in place could have created the consumer trust we need by giving everybody rules to live by. Privacy laws can address emergencies. If we had a privacy law, it could not only govern data use in ordinary times, but it could set rules for emergencies.

WILL DEVRIES: Jessica, I couldn't agree more. I think if we had a comprehensive privacy law in place that helped improve trust in the entities that are doing this and a sense of how the data was going to be handled, people would feel better both for this crisis and for the next ones that I'm sure we have in front of us. This is imperative for us to think about as we rely more and more on digital services to handle aspects of our lives, including public health responses.

AARON BURSTEIN: To stick with that comparative perspective, other countries have certainly done testing differently and have different privacy regimes. Bill, do you have observations about where technology-assisted efforts to stop the spread of coronavirus have functioned better, and are there any lessons that the United States could learn from those examples?

WILLIAM McGEVERAN: I think that Jessica's point about having the legal infrastructure in place is really illustrated well by the experience with contact tracing generally, including its integration of technology but also including just the flow of information from a test, through public health authorities, through contact tracing, and through subsequent isolation.

All of that has worked better in other countries. There are a lot of reasons for that, but one of the reasons is that in Europe and in a lot of the Asian countries that had

aggressive early responses involving testing and contact tracing, they had the kind of legal rules in place in advance that made it clear how personal information could be handled. Some of the same problems with uptake of technology have happened in other places as well, but I think other cultural differences also help explain that.

The greater success in contact tracing elsewhere is partly attributable to the better and more comprehensive privacy law in those places—"comprehensive" being a really important word here, and Jessica and Will both used it. Even a lot of the fairly broad privacy laws we talked about at the beginning of our conversation would say nothing about the handling of this kind of public health data, because they are really pretty consumer-focused. We are a long way from having the sort of "all subjects, all sectors, rights-oriented" legal regulation that other countries do.

AARON BURSTEIN: Let's shift to the protests that followed the death of George Floyd and other Black citizens at the hands of police. Alex, have you seen any privacy issues arise in either the government's response to the protests?

ALEXANDRA GIVENS: Yes. We talk a lot about the importance of the First Amendment in this country and the right to peaceful assembly, and a vital element of that is that people feel able to come together and protest without being targeted by surveillance, or worried that their presence at the protest is going to be revealed or prompt retaliation.

Technology is really changing law enforcement's capacity to monitor protests. Drones flew over protests in Minneapolis and New York; a government spy plane flew over protests in Washington, D.C.; video camera feeds can now be analyzed with facial recognition software; law enforcement can use signals from your cell phone to follow your movements. Even for people who don't attend a protest in person, technology allows law enforcement to monitor social media posts for organizing behavior, for example. The use of all of these technologies at peaceful protests in my view really does cast a troubling shadow over constitutionally protected activity.

I think a crucial point that often gets missed here is that that doesn't just matter for the protesters. The protests are prompting a nationwide conversation that is long overdue about systemic injustice. So the right for people to come together in this way matters for broader society, for changing conversations in companies, in civil society organizations, and in the halls of government too.

More granularly, the biggest problem is that we know the effects of government surveillance are felt most strongly by marginalized communities. These problems can be seen literally in the technology—for example, research showing that facial recognition technology works less accurately when identifying people with darker skin tones. But there is also increasing use of data analysis to inform policing—predictive policing based on location-based trends analysis, for example—and again, research shows that that often targets minority communities.

Those systems are all fed by surveillance activity. As the police track protest organizers or identify hotspots or analyze active hashtags on Twitter, they risk, ironically, feeding into the exact same systemic inequity that is the very subject of the protests. As a society, we're asking Black protesters not only to carry the heavy weight of leading the national conversation, but also to risk long-term and disproportionate exposure as they do so. Those are some of the real concerns that we are focused on. As we grapple as a country with these questions of systemic inequity in our system, how is surveillance technology potentially deepening and contributing to those problems?

JESSICA RICH: Can I just add that one interesting point about this challenge is that cell phones and other technologies have also enabled citizens and protesters to document instances of abuse. We saw what happened to George Floyd, and that the police lied about it, because individuals captured the events on their cell phones. So this makes the issues more complex to tease out.

Again, this is yet another reason why we need stronger laws—to have clear rules about what kind of technology can be used at these protests, and then, if something is recorded, how those recordings can be used and stored, etc. Some cities have enacted laws here, but it is pretty scattershot and hardly widespread or uniform.

WILLIAM McGEVERAN: And let me just add one more brief point to Jessica's: not only has new technology helped document things as she says, but technology is also one of the drivers for organizing all of the assemblies Alex was discussing. I went to a protest after George Floyd was killed, and where did I learn about it? From a Facebook group that I follow, that was narrowcasting information to people like me who shared those interests and who were likely to show up for a protest.

It is dangerous to point to technology as either the villain or the angel in these discussions. It is about how we regulate that technology in all directions.

ALEXANDRA GIVENS: One interesting trend is the increasing movement towards community engagement around how technology is used by law enforcement, and I think that is a critical piece of this conversation. You can see this in ordinances at the local level against police use of facial recognition technology, for example—or, even apart from that, an increasing focus on how to reestablish trust between law enforcement and the community that they are there to protect.

That important trend needs to continue to help people feel more buy-in and understanding as to why certain

technologies are being used, and then, when they are concerned about the disparate manner in which surveillance is happening, to be able to push back and have their voices heard in that conversation.

JANIS KESTENBAUM: We are going to move onto privacy developments in Europe. Just a few months ago, the Court of Justice of the European Union (CJEU) handed down a landmark decision in the *Schrems II* case. Bill, could you start us off by giving us an overview of what the case is about, what the CJEU decided, and in the short term what impact it is having or is likely to have on American businesses?

WILLIAM McGEVERAN: The decision is very complex and very technical, but it is relatively easy to sum up in overview form. The quickest overview of *Schrems II* is that it is the Court of Justice of the European Union saying, "We meant what we said in *Schrems I*." *Schrems I* was a challenge to the movement of personal data of EU persons to the United States under what was then the most commonly used arrangement for those transfers, the U.S.-E.U. Safe Harbor Agreement. The Court said that the Safe Harbor Agreement did not do enough to constrain the U.S. government, particularly intelligence collection of information about EU persons from American companies that were holding it. So the court said the Safe Harbor was inconsistent with EU law, and invalidated it.

The response of our government and the European Commission, which is sort of the executive branch of the European Union, was to create a new agreement called the E.U.-U.S. Privacy Shield. It made some changes, but they were not really for the most part changes that addressed what the Court had talked about in *Schrems I.*

The challenge worked its way back up, and *Schrems II* is a decision that says, "The Privacy Shield, like the Safe Harbor, did not do very much to constrain the U.S. government from obtaining data about EU persons that would be transferred to U.S. companies and held by them; so it too is invalid." So *Schrems II* explicitly invalidates the Privacy Shield—which leaves us to wonder what the name of the third agreement would be; would it be "Privacy Armor" or whatever wording they come up with. Whatever you call it, the architecture of it was not satisfactory to the European Court.

But actually, in substance, all of the concerns the court stated are equally true of every other mechanism for transatlantic data transfers. Some companies have been relying on model contract clauses, which is another way E.U. law allows international data transfers. Some have adopted so-called "binding corporate rules." None of these things constrains the Department of Justice or the National Security Agency or any other U.S. law enforcement or intelligence authority from getting information from private companies in the United States. So my read of *Schrems II* is that all of those other mechanisms are legally suspect as well.

Where does that leave U.S. companies? In quite a pickle, because it is not clear how the European Union and the United States can negotiate their way around the structure of U.S. law enforcement and intelligence access to privately held data here in our country. Unless we are ready to really revisit that, it puts a lot of the trade in data between Europe and the United States in peril.

JANIS KESTENBAUM: Bill, a follow-up question. As you indicated, the Court flatly struck down the Privacy Shield. You mentioned two other transfer mechanisms: binding corporate rules and model contract clauses. What did the CJEU say about whether companies can continue to use them, including in transferring personal data to the United States?

WILLIAM McGEVERAN: The Privacy Shield aspect of the ruling was very explicit and clear. The rest of it was less clear and is subject to some amount of interpretation by different lawyers. Reasonable minds can differ about exactly how bad the *Schrems II* opinion is for those other transfer mechanisms. For my part, I think it's really bad and I would expect a future *Schrems III* decision to use the same logic to invalidate those as well.

But different companies are reading the tea leaves in the very long and complex opinion to try and see if they can find their way towards legitimate authorized transfers of information to the United States. The Court might have served both governments and businesses better if it had gone ahead and made a more clear, broad ruling because we would have known more certainly where we stand.

My own view is that it's only a matter of time before the Court would say in *Schrems III*, "Yes, we meant what we said in *Schrems I and* in *Schrems II*: If the information is accessible to your government without these safeguards listed in European law, then it cannot be transferred."

JANIS KESTENBAUM: I gather you think that in just a couple of years we'll have a *Schrems III*?

WILLIAM McGEVERAN: That's my view, yes. The Court does not appear to be terribly concerned about the enormous practical difficulties this unleashes—not just for American businesses, but for European businesses and governments. The CJEU does not occupy itself with that part of the problem. That is a political problem, and the judges essentially say, "Work it out if you can, but here is what European law says." This is going to be a very thorny problem to work out in the coming years.

JANIS KESTENBAUM: Alex, as Bill just pointed out, to address the Court's concerns would require reform of the U.S. national security and surveillance laws—at least that's one interpretation of it. In your view, is there any short- or medium-term paths to legal reform in the United States that could accomplish that?

ALEXANDRA GIVENS: This decision really is a wake-up call for policymakers and the intelligence community. In our view, stronger privacy protections have to be built into intelligence surveillance authorities. You can try to look for commercial quick fixes, but the problems we are talking about are systemic and really do look to how law enforcement is accessing data.

We have long talked about surveillance reform as a human rights imperative, but *Schrems II* really drives it as an economic imperative as well, for businesses to be able to keep operating. There are two core concerns raised by the decision. One is that too many Europeans are subject to data collection—this is the "proportionality of the surveillance" piece of the conversation. Another issue is affording Europeans meaningful redress.

We've called for some steps for Congress to address these. For example, prohibiting upstream surveillance through which the U.S. government temporarily seizes virtually all internet-based communications flowing into or out of the United States. We have called for strictly limiting the purposes for which the U.S. intelligence agencies can obtain personal data under Section 702 of the Foreign Intelligence Surveillance Act, and also establishing stronger constraints on U.S. officials' ability to gain access to and use that data.

Then there is the question of how you create a mechanism of redress for people whose rights have been violated. That's a thorny question that the legislators will have to navigate.

WILLIAM McGEVERAN: Let me just add one other thought in response to Alex. If we did make the adjustments necessary to satisfy the European Court as to the rights of European citizens, I think it would be politically and perhaps constitutionally impossible not to completely overhaul the way we handle data of U.S. citizens as well. Although the Europeans are perfectly neutral on how we handle data about our own American citizens, the reality is that it would have to be a more comprehensive approach and not just one that was targeted at only helping Europeans and not U.S. citizens.

JESSICA RICH: On the national security side.

WILLIAM McGEVERAN: Agreed, yes.

JESSICA RICH: On the commercial side, the Safe Harbor and the Privacy Shield have always included requirements that go beyond U.S. law.

To that point, I would add that I was at the Federal Trade Commission when both the Safe Harbor and Privacy Shield were negotiated and enforced, and there were many new requirements that the FTC and the Department of Commerce agreed to with respect to the protection of personal data on the commercial side. But the challenge and dividing point has always been the national security use of data. There was always the sense that "We can pledge to do this, that, and the other thing on the commercial side, but if they can't solve the national security issues, the program is not going to succeed."

WILLIAM McGEVERAN: Right. You could make the commercial privacy elements that were present in Safe Harbor and Privacy Shield much, much stronger, but the CJEU simply would not care, as long as the U.S. government had access to Europeans' personal information.

JANIS KESTENBAUM: As Bill aptly said, this puts everybody in a pickle, no one more so than U.S. companies. So, Will, what can they do, given that they do not have the ability to force the U.S. government to change its national security laws and practices or provide a mechanism for redress?

WILL DEVRIES: There is not much that companies can do, even the largest companies like Google. This is a political question about the application of surveillance law and it needs a diplomatic solution. I agree with what Bill and Jessica said, which is there is no guaranteed commercial privacy or commercial solution that obviously addresses the issue.

This is a big deal. This could leave all U.S. companies that have business in Europe—which is essentially every online company—without a viable mechanism to transfer data to the United States. That means trillions of dollars in transatlantic trade, and thousands and thousands of companies from all industries, all sizes—technology, financial services, health care, transportation—every sector you can think of.

And not only is it about EU-to-U.S. transfers, but most U.S. companies were relying on the Privacy Shield for onward transfer to third-party countries. The ruling mandated that companies perform an assessment of national security laws and judicial redress in any country where data may be transferred, so it has big global implications for data transfers to anywhere around the world, not just the United States.

So what are companies doing? Companies seem to mostly have done what we have done at Google, which is to just have faith in the process, stop transfers via Privacy Shield, and engage with customers and governments to institute alternative mechanisms like contracts.

There is work bilaterally to address this between the European Commission and the U.S. Commerce Department. We need them to take steps on both sides and act with urgency. We need European stakeholders to give clear guidance about what to do in the short term, what is safe to rely on for now. And we need the United States and its government to address surveillance reforms in a direct and concrete way.

The surveillance authorities that European governments have are similar to the surveillance authorities in the United States, so this is not an issue about one country being that far from the others. There are other countries in the world

that have rule of law and due process issues that put them far apart from the U.S. and E.U., so there should be room here for agreement. We just need the U.S. and E.U. to come to the table and agree.

And, I think, comprehensive federal privacy legislation is going to help create an environment for a durable agreement on transfers of data between the European Union and the United States, so I would urge them also to keep going on the momentum toward comprehensive privacy legislation in the United States.

AARON BURSTEIN: One of the concerns that surrounds *Schrems II* and has surrounded GDPR before that and the Data Protection Directive before that is data localization, at least at a de facto level—that is, restrictions on where companies can send and store personal data. Will, looking at Europe and beyond, where are we are seeing data localization requirements, and what are some of the underlying forces that are behind those requirements?

WILL DEVRIES: We are seeing this come up a lot. This is a very concerning global issue.

Data localization, I think, is one manifestation of the desire for local government control over the offering of online services that have become such a deep part of our lives and our societies. I think the *Schrems II* decision is one reflection of that and we are seeing data localization proposals as another manifestation of that.

India is probably the most prominent example, and it continues to flirt with requirements in its pending national privacy law around data localization. What seems to be animating a lot of that concern—and we've seen this in other countries as well—is a desire to have direct access and direct control of user data for law enforcement and local compliance purposes. The view is that data is a domestic asset that must be controlled by domestic entities. Countries might have different structures in terms of content requirements, legalities, and the terms under which service is offered, and they think that they will have more control of those if the data is actually held locally.

There is also some belief—which I think is mistaken, but it comes up a lot for developing countries—that if they require data localization, there will be more local infrastructure investment or that local providers will receive more business, spurring domestic job growth. In most cases, we have had success when we explain why that is not really the case, that locating a server farm is not the kind of sustainable economic development that they are looking for.

I think these initiatives are part of a general trend for governments to reassert their participation in the way that services are offered in their countries, and that spirit is very legitimate. It is something that while the internet was in its growth phase didn't really occur too much; it was really a U.S.-led and Western-led internet and it just sort of arrived in other countries without a lot of direct interaction with those governments. That is changing, and I think that is a very understandable and reasonable goal.

But I think we have to be very concerned about how this legitimate concern manifests in terms of data localization and bans on transfer of data because the cost of compliance, the splintering of policies, the splintering of services globally, could make things very hard for consumers and very hard for industry.

AARON BURSTEIN: For a long time the U.S. government has been a staunch opponent of any sort of data localization requirements and has been a proponent of maintaining the free flow of data across the globe. Recently—and we are still in the middle of this process—the Trump administration has taken action against TikTok and its owner, potentially including a ban on offering the app in the United States unless parts of the company are transferred to a U.S. owner, or other control is transferred. Bill, do you think this marks a watershed in U.S. policy surrounding data localization?

WILLIAM McGEVERAN: I think, consistent with what Will was saying, that we have seen an evolution towards a more fragmented regulatory approach to the internet everyplace in the world for a host of reasons—whether it is less democratic regimes trying to exercise political control, or whether it is the privacy concerns that we see driving *Schrems II*, or whether it's economic or global competition motivations.

The TikTok controversy is definitely another step on the road away from what used to be a broadly agreed-upon principle that a unitary global internet was important—and, in some people's eyes, inevitable, unstoppable. Instead, national lawmakers have asserted themselves to apply their national law to global information flows.

Without going into all the details of the TikTok case in particular—I think there is a lot of controversy about the mechanism the government is using here and disputes about the degree of the security threat—there is also a recognition that, in a world where foreign intelligence agencies are interfering in American elections and there are enormous concerns about surveillance and espionage, the United States is not going to be accepting all global data without restraint.

I hope we are maturing to a more sophisticated global internet that balances the virtues of having unified worldwide services with legitimate interests of individual countries. That process will involve a lot of growing pains and we will have missteps along the way. So yes, I think that TikTok is an important development, but it is one in a series of things that have been happening over time.

AARON BURSTEIN: Another effect of privacy and data protection laws has to do with how they might affect competition. One of the concerns that has surrounded the GDPR, and we are also hearing it in connection with the CCPA, is that they may favor certain models of collecting business data and the business models that are associated with those

types of data collection. Will, could you give us an overview of what those concerns are and what companies stand to gain or lose under the GDPR and CCPA?

WILL DEVRIES: Yes, and I'd love to hear from others as well as to what they are hearing. I have been paying a lot of attention to this issue over the last several years, obviously thinking about this from the perspective of Google, but also as somebody who has worked in privacy law for many years and seen the evolution of it.

There is, I think, an increasing awareness that privacy laws in their basic structure often favor certain relationships over others. In particular, first parties—who have a direct relationship to users, collect data because users come to their services to use them in a deliberate way. These entities are more able to collect permission from users or establish the conditions under which they can process that data under the law, versus parties that rely on a third-party relationship and have to obtain the data via some other mechanism. Third parties also can have a more difficult time with notice, consent, and other obligations imposed by law under GDPR as well as under CCPA.

I think that for those of us who understand privacy and were looking at those laws as they were designed, it makes a lot of sense–that's honoring consumer expectations; that's the way consumer privacy law was designed.

We also see similar concerns being raised around unilateral changes that some companies are making. As privacy becomes a big brand driver—certainly we see it with Apple, Google, and other players—we are seeing major changes that are increasing privacy offerings for users and protection of their data, minimizing the amount of data collected, and adding restrictions on platforms that restrict how data can be used. Apple's new restrictions on the advertising identifiers on iOS is a current example of that. In response, other companies that use that data are raising a point about "Well, that's going to make it harder on a smaller player, as a player that operates on those platforms."

Those are very interesting privacy issues and intersect with competition.

We have also seen the flip side of that concern. For years we have heard people express concern that market power may lead to abuse of consumer privacy, to less protection for consumer privacy. We have seen that come up recently in the German competition authority raising this with respect to Facebook.

I think there is a general recognition that those concerns are best addressed by privacy law, rather than competition law.

We are going to be seeing this issue over the next several years as both competition and privacy regulators work trying to solve it. I would hope that they can work in a cooperative way and that they can each in their own sphere of influence understand what the other is doing and try to come to some consistent outcomes. I think they need to, in order to navigate these issues.

JESSICA RICH: I agree with what Will said about the laws favoring larger established platforms; both GDPR and CCPA do so for a few reasons. One is just cost. The larger companies have more resources to analyze new requirements, implement new processes like providing access and choice, perform risk analyses, and document everything. Many large companies seem very comfortable with GDPR and CCPA, relative to the smaller ones; also, since GDPR was adopted, the market share of some of the big platforms has grown while some small companies have actually pulled out of Europe.

A second major reason is the focus on third-party sharing. Cutting off third-party sharing, a particular focus of CCPA and other state proposals, favors larger companies because they keep many of their functions in-house, while smaller companies often rely on other entities to perform every day, basic tasks.

The irony, of course, is that a law that mostly focuses on data sharing allows companies that don't share data to do almost anything with it. But I would say two things about this: One is that laws that impose more substantive privacy requirements on anyone that collects, stores, or uses consumer data, and do not focus so much on third-party sharing, might be more helpful in equalizing the playing field between different business models and entities.

Second, I think the FTC, as both a consumer protection and competition agency, needs to provide more transparency about the relationship between consumer protection and competition and even make recommendations to Congress if needed to address the different concerns. Some people think that privacy and competition are irreconcilable because of some of the issues we've discussed, but I think the FTC is in a unique position to provide more transparency and leadership around these issues.

WILL DEVRIES: To second that, the FTC is in a great position. Something that I have always appreciated about the perspective of a consumer protection regulator is they get to look at both the market conditions with a competition lens as well as the data privacy and data protection lens. There can be a gulf when you have two different regulators, as we see playing out occasionally in Europe and in other jurisdictions.

One great fear of mine is that people will lessen their support or feel like we cannot pass a federal law because they are concerned about the impact on competition. But I think you can solve that.

There are some competitive impacts of a privacy law that are inevitable, such as that first-party relationships will have a competitive advantage and better consumer understanding than third-party relationships. But there is a lot in terms of compliance burdens, coverage, and scope that must be carefully crafted to avoid creating a disproportionate impact on certain businesses.

So you can be smart with principles-based legislation that takes into account the scope and resources of covered

businesses and organizations, and I hope people don't get scared off of privacy law for that reason.

JANIS KESTENBAUM: That's a good segue to what the FTC's recent activity in the privacy sphere, where it has taken substantial action recently by reaching significant settlements with Facebook and YouTube; opening a major rule, the Children's Online Privacy Protection Act (COPPA), for review ahead of schedule; and implementing revisions to key provisions in its consent orders in response to the Eleventh Circuit's decision in *LabMD.* Jessica, what's your assessment of these developments?

JESSICA RICH: I think it is fairly clear to everybody by now that the FTC needs stronger laws and more resources to be a truly effective enforcer and regulator in privacy. But as it is, with a few dozen attorneys, a general-purpose law that was drafted in 1914, a few sector-specific privacy laws, and very limited rulemaking and civil penalty authority, the FTC has managed to become the main privacy agency in the United States—and indeed, probably the leading privacy enforcer in the world. Nobody handed this to the FTC—there is no overarching privacy law that Congress enacted and assigned to the FTC. But the agency has nevertheless developed an enormous body of work stopping privacy abuses and protecting consumers.

Through that lens, I would say that the FTC is doing a great job of using and pushing the authority it has to protect consumers and respond to developments and setbacks.

On the *Facebook* front, the FTC obtained a groundbreaking $5 billion civil penalty and injunctive relief that fundamentally changes the way the company manages privacy. The settlement has been criticized—$5 billion wasn't enough—but I don't see other countries imposing a $5 billion fine on Facebook for privacy violations. Also, Mark Zuckerberg was not named personally in the complaint, but he is on the hook in many ways throughout the order, and he will be subject to an order and penalties for future offenses. The FTC wouldn't be able to get this type of relief in litigation.

YouTube is in many ways even more interesting. Basically, the FTC crafted a way to raise compliance across the whole platform—Will knows a lot about this, I'm sure—without suing hundreds of the little channels on the platform, which would be very difficult and politically fraught.

Critics would have liked to see stricter requirements forcing YouTube to affirmatively investigate and take responsibility for all content on the platform, and maybe Congress will decide to change the law and impose that requirement. However, because YouTube in this situation is currently subject to an "actual knowledge" standard, it is highly unlikely that the FTC could have obtained this type of relief in litigation.

The COPPA review and the new consent language are examples of the FTC responding to developments and setbacks. The FTC needs to review COPPA regularly to keep pace with technology, and many issues have arisen since the last time the COPPA Rule was reviewed in 2012. That's a long time in the online world.

Finally, in light of the Eleventh Circuit's decision in *LabMD*, it was absolutely necessary for the FTC to revise its standard order language in data security cases. In ruling against the Commission, the Eleventh Circuit sent a very strong message to the FTC that the consent language it had been using for 20 years was "unenforceably vague." As a result, the FTC developed fairly swiftly, and has now obtained in various settlements, order language that is far more specific. We will see how this new language fares over time.

JANIS KESTENBAUM: Jessica, looking forward, whatever the result of the presidential election, we may have a new Chair of the FTC in the not-too-distant future, and that individual will face significant national and international challenges. What do you recommend that they focus on in the privacy area?

JESSICA RICH: The most important thing the FTC has to get through in the near term is the challenge to its Section 13(b) authority, which is currently before the Supreme Court. If the FTC loses, it will not be able to go directly into court to get consumer redress, which is a core part of the agency's ability to protect consumers. This has more to do with privacy than you think. Privacy cases are often administrative, but not always, and wherever possible, even in privacy cases, the FTC will seek to get money back for consumers.

Second, the FTC brings most of its fraud cases under this authority, and many or even most of these cases involve some sort of data misuse. Curtailing the FTC's fraud authority could also increase fraudsters' ability to misuse information.

And of course, if the FTC loses this case, it may need to shift more resources to its fraud program, since obtaining redress will require multiple steps and will be that much more difficult.

But beyond the 13(b) issue, the FTC should be focusing intently on updating its authority and tools to meet today's challenges, especially those posed by technology. This means pushing even harder and more aggressively for stronger privacy laws and more resources, and maybe even drafting a model law and saying, "This is what we think a law ought to look like."

Relatedly, the FTC should consider public workshops to discuss the areas of divide (preemption, private right of action), which most people just keep talking about without proposing good solutions.

Also, the Commission's Unfairness Statement and its narrow concept of harm really hobbles the FTC. The agency should consider issuing a new policy statement, perhaps just on the issue of privacy harm, to update its thinking and

provide guidance. Remember, the Unfairness Statement was drafted in the 1980s, long before we had the internet, mobile devices, apps, social networks, health websites, etc. Its discussion of harm reads that way.

The FTC also needs to beef up its tech expertise. For example, it has a lot of trouble attracting technologists, in part due to outdated ethics restrictions that need to be updated and tailored to the use of technologists.

In addition, Commissioner Slaughter has talked about using the Magnuson-Moss Warranty Act in privacy. I think this would be very hard, even impossible, in privacy writ large. However, maybe the agency could bite off a narrower issue (data security?) to tackle using this authority.

Last, I think the agency could take a more strategic approach to working with other agencies that have legal authority the FTC lacks. In *Equifax,* for example, the FTC worked with the Consumer Financial Protection Bureau and was thereby able to obtain civil penalties not otherwise available to the FTC. Unless and until Congress beefs up the FTC's authority, the agency should look for additional opportunities to team up with other agencies that have complementary authority.

AARON BURSTEIN: As the year draws to a close, it looks like 2020 will not bring the kind of comprehensive federal privacy legislation that Jessica and others have alluded to throughout the conversation. But there has been a really unprecedented degree of activity on this issue over the last two years in Washington, including a notable development recently with the introduction of the SAFE DATA Act by Senate Commerce Committee Chairman Senator Roger Wicker. Jessica, could you tell us where we have seen bipartisan agreement develop, and is there a set of issues that look like they are on the road to resolution at this point?

JESSICA RICH: From reading the bills and watching some of the hearings, there appear to be huge areas of agreement that have never existed before, though there are also many areas of separation.

First of all, everyone thinks there ought to be a law, which is huge. Also, every bill has a set of consumer rights—some form of notice, access, correction, deletion, portability, special treatment for sensitive data. Of course, the definitions and terms differ, but this is progress.

The bills also all include business responsibilities—some form of data minimization, data security, third-party oversight.

Putting preemption aside, which is one of the big areas of disagreement, there seems to be agreement that the states should at least be able to enforce a federal law.

There is even agreement—with slight differences—that the law should cover data that is linked or "reasonably linked" to an individual, which used to be controversial.

There is also lots of discussion about the need to move beyond notice and choice, although unfortunately, most bills don't actually do this. Instead, they still largely revolve around notice and choice, which puts the burden on consumers.

AARON BURSTEIN: You mentioned preemption as one of the areas of disagreement, and a private right of action also seems to be part of that. Is that divide as unbridgeable, or is there a way forward to some sort of resolution?

ALEXANDRA GIVENS: First, to build on Jessica's response, I think there has been a remarkable coming together, over the past year in particular, with ideas that previously were dismissed as radical now becoming mainstream, which I think is really a positive sign.

One of the pieces I will add is an increasing recognition of the need to deal with discriminatory uses of data and to fold those concepts into the bills. It is nice to see even some bipartisan recognition of that, although it is the Democratic bills that have really advanced that as a priority.

Preemption is a deep sticking point, of course. CDT is in a small minority that has said that well-crafted preemption may be acceptable *if* federal standards are strong enough. But, as states like California and elsewhere pass their own measures and show the ability of states to drive the national conversation, that sets a higher bar for federal privacy legislation to have to clear to get that type of buy-in.

CDT's Director of Consumer Privacy, Michelle Richardson, has smartly observed that this debate is becoming perhaps overly entrenched in terms of the impact of preemption. Companies are talking very loudly about the "patchwork of states' laws" that could result without preemption, but realistically it is hard to see that emerging if there is a sufficiently strong federal standard. It is hard enough to get state laws passed, and if there is a strong federal bill filling that space, even without preemption language, I think it will take away a lot of the energy for further incremental change.

On the other side, consumer groups say there should be no preemption because we need state innovation, but the reality is that if there were a strong federal law in place, regardless of whether it had preemption language in it, it probably would dissipate a lot of states' energy. So the issue might not be as high-stakes as it is made out to be.

On the private right of action, the conversation there right now does feel equally tough. A private right of action is an important mechanism for securing consumer rights.

It is an important addition to the enforcement power of State AGs and the FTC, which we know tend to be limited through resource constraints, and also by political elements. When you look at the arc of the law and how enforcement trends over time, state AGs and regulatory agencies have limited capacity and political will, so there is a significant role for consumers to play in vindicating their rights.

Having said that, how do we get there? This is another area where the conversation may not need to be as polarized as it is right now. Right now a lot of the conversation

is "private right of action or nothing," and this myth that "we either have to deal with the risk of a massive upsurge of litigation from the plaintiffs' bar or no private right of action at all." In truth, there are dials you can tinker with in a private right of action to mitigate some of the risks people are worried about. You can have thoughtful conversations about "What's the relief? What's the legal standard of proof? How do attorney's fees work versus punitive damages?"—those types of issues.

There is room to have conversations around each of those dials, and that conversation needs to be happening now, so we can pick up momentum again in the new Congress to drive this effort forward.

JESSICA RICH: I think you are right that there are middle grounds on all of these things. But, right or wrong, it is the desire to preempt state laws and stop private rights of action that brought many businesses to the table. They would have to see the value of a law beyond those two issues in order to want compromise, and I don't know that we are there yet.

WILLIAM McGEVERAN: I 100 percent agree with everything Alex and Jessica said about this. I'd mention one example: Cameron Kerry and his team at the Brookings Institution released a report this summer, called "Bridging the Gap," and it talked in detail about some of the creative uses of those dials that Alex was alluding to.

But what will most likely break the logjam around these issues will be a political shift towards the imperative to get a bill done. To some extent, preemption and private rights of action have become excuses for not moving forward with a serious discussion. As soon as everybody gets serious and decides it's time to move, some of the middle grounds that Alex talked about and that the Brookings report talks about would suddenly appear really attractive to everybody.

WILL DEVRIES: I will put in one note looking at this from the side of industry. There is unbelievable alignment around the need for privacy law. Something I'm shocked to see after working in this area for so long is that businesses have come to the table—even the Chamber of Commerce and groups that you would have never expected to be there. And they are there because they understand (1) the trust and brand issues at stake, that they need to establish trust in order to smooth the wheels of commerce on the internet and in the data-driven economy generally; and (2) they are there because they are—rightly—worried about the splintering of compliance obligations across 50-plus jurisdictions in the United States. That is a real threat to the ability of these companies to operate, and especially for smaller companies to be able to have a prayer at having a reasonable compliance strategy.

To the extent that federal law is going to address that, preemption has many flavors. So, as Alex was mentioning, there is likely a way to craft preemption that addresses the compliance and operational concerns raised by businesses while preserving room for states to still be the laboratories of experimentation within that rubric of a standardized nationwide compliance standard.

AARON BURSTEIN: This has been an extremely illuminating discussion. Is there anything else you'd like to tell us before we wrap up?

JESSICA RICH: I don't think we missed it, but almost every topic we discussed pointed in the direction of needing stronger privacy laws in this country, and particularly a strong federal privacy law. I thought that common theme was great, that we were all pointing in the same direction, despite our different perspectives and backgrounds.

WILL DEVRIES: Having worked for almost 20 years as a privacy professional, I couldn't have imagined that it would become a global policy issue and front of mind in political debates and international trade the way it has. It's wonderful, but I hope that that energy can lead to some really good policymaking.

I think that we have an opportunity here. Just like back in the early 1990s during the Clinton administration, with the steps they took to establish the commercial internet, we are at that same precipice where we get to decide what the future of the data economy is.

ALEXANDRA GIVENS: I will add, in a very similar vein, this is now a kitchen table issue. This is something that consumers care about. They know it affects them.

The impact has been driven home now more than ever with the COVID-19 pandemic. Something as simple as the Web searches in your browsing history can reasonably indicate a positive COVID status—something that may well be a preexisting condition for insurers going forward. People know the stakes of why it's important to protect their information.

My hope is that lawmakers pick up on the momentum of this year and really carry it forward next year—that we don't lose the progress that has been made, but instead lean into this opportunity and get it across the finish line next Congress.

WILLIAM McGEVERAN: I agree that this has become such a politically salient issue and, as Alex said, a kitchen table issue. It makes this a great moment for increased creativity in thinking.

A lot of us referred to the fact that lots of these different proposals are trying to innovate in a lot of directions. At the same time, sometimes they do still seem to be anchored to ideas that we all have reason to be skeptical about, particularly things like notice and consent. I was on a panel recently where David Medine said, "Consent is dead; get over it," which I thought was a great twist on an old privacy aphorism that we all know.

As we consider what privacy law ought to look like, we are freed up to look into the future and not just the past and to recognize that some of the ways that we have talked about privacy were great for the toddlerhood of the digital economy but not for its adolescence and its adulthood. I hope we can grow into thinking about privacy more broadly, with an eye toward the serious harms that individuals experience, and the need for a real sense of stewardship by data collectors, all while facilitating continued growth and innovation.

AARON BURSTEIN: On that hopeful and appropriate note, we will wrap things up. I thank you for your time and your thoughts.

JANIS KESTENBAUM: Thanks to you all for participating. ■