All right John, we're free to go. Good afternoon. On behalf of the American Geographical Society Council, our members, and the staff,
it's my pleasure to welcome you to this sixth Location Tech Task Force Blue-Ribbon Panel, Legal Perspectives on Mobile Location Technology. To those of you participating in the conversation on WebEx, and those that are watching our live stream on Facebook, it's
great to have you joining us this afternoon. We are proud to partner our EthicalGEO initiative with the Henry Luce Foundation
to investigate the societal implications of geospatial technology and location tracking. Mobile location-based applications have become ubiquitous in our society. As all of
you know,
they have changed the way we live our lives in a very short period of time.
There are, however, problematic and unanticipated effects of using this technology. To better understand the ethical implications of its use, we have provided this platform to frame the discussion and to address these issues as they are already impacting our lives on a daily basis. COVID-19 has put a spotlight on the concept of using mobile tracing and surveillance to fight the pandemic.
Over the past several weeks, our first five Blue-Ribbon Panels met and looked at ethical implications of mobile location technology and the impact on vulnerable publics from an international perspective and from the unique American experience.

In addition, we had a panel of national security leaders, who focused on mobile tracing technology, and it’s used in national security and democracy.

We also heard from state and local leaders who shared their invaluable experiences with us, and just a couple of weeks ago, we looked at data quality and building trust, false negatives, false positives and policing / surveillance.

In the case of all the panels, the discussions have been fascinating and comprehensive.

We also had the opportunity to hear from Ambassador Samantha Power, and she added the human rights aspect of the use of mobile technology.

Other leadership spotlights investigated digital contact tracing tools, as well as technology and LGBT+ location privacy during COVID-19.

Today, we turn our focus to something that will affect all of the groups we have spoken to over the past few months, and that is the legal issues involved with mobile location technology.

All of this testimony that we have collected through the Blue-Ribbon Panels and the Leadership Spotlight testimonies will serve as the basis of information and data that policy makers will use to help guide us in the future.

Before we move on, I'd like to explain to those of you on our WebEx platform, the best way to get the most out of today's panel.

For those viewing on desktop computers or laptops, we recommend that you customize your viewing by hovering the mouse in the top right of your screen and selecting the icon in the middle.

During our Q and A session later, to ask a question, hover your mouse under the arrow and click on the question mark icon in the gray bar at the bottom of your screen.
For those of you using a tablet or mobile device, select the icon with the three dots, which will then allow you to select the question mark icon to submit your questions to our panelists.

And now, it's my pleasure to introduce Dr. Christopher Tucker, the Chairman of AGS, and our moderator for today's session. Chris, it's a pleasure to welcome you and your panel.

Thanks

John, and thanks to the team for all the work to get this organized today. AGS has a proud history of 169 years of convening government, industry, academe, and the social sector around the vital issues of the day through a geographic lens.

Last year, we began our EthicalGEO initiative looking at the ethical implications of mobile location technologies, geospatial technologies and with the dawn of COVID-19, we built a partnership with the Henry Luce Foundation, which has created this Location Tech Task Force and the Blue-Ribbon Panels that we've convened up until now. We could not be more proud to have these three world experts with us today.

And before we begin their presentations, I'd like to give a short introduction of each of them. Ms. Stacey Gray, Senior Counsel at Future of Privacy Forum (FPF), focuses on issues of data collection in online and mobile platforms, ad-tech, and the Internet of Things. At FPF, she worked on FCC and FTC public filings, and publishes extensive work related to cross-device tracking, smart home technologies and federal privacy.
regulation and enforcement. She also is a certified information privacy professional. Mr.
Kevin Pomfret is a partner at Williams Mullen. He represents a wide range of public and
privately held companies and counsels companies on technology, joint ventures and
software and data licences. Kevin serves as the co-chair of Williams Mullen’s unmanned
systems and data protection cybersecurity teams. As a former satellite imagery analyst
in the intelligence community, Kevin is also a thought leader in geospatial technology
with almost 30 years experience in the geospatial community. In addition to his legal
representation, Kevin founded and is the Executive Director of the Center for Spatial
Law and Policy. And Mr. Jacob Snow is Technology and Civil Liberties Attorney at the
ACLU of Northern California where he focuses on consumer privacy, government
surveillance,

and the preservation of free speech online. Jacob works in the courts and legislature to
protect people’s privacy from intrusion by both companies and the government. Before
joining the ACLU of Northern California,

he was staff attorney in the San Francisco Office of the Federal Trade Commission.
Thank you to all three of you for joining us today.

I know that you all bring very valuable and very different perspectives to the table on
the implications of mobile location technologies in an era of COVID-19, and also for their
implications beyond COVID-19.

One of the themes that we’ll have in our panel today is how new technologies, new
systems, new laws, new bureaucratic institutions are put in place in response to a
particular threat

and often stick around as we find ourselves in the face of a new one, and as we often
don’t have the opportunity to take the time and think through the ethical implications
of those beforehand. And with you three here today,

I know we’ll have plenty of time to reflect on all of that. So, thank you again for joining
us, and Stacey, if you’re ready, we’ll hand over the microphone to you to kick us off.

Great. Thank you so much Chris. Wonderful. Yeah, that was an amazing introduction,
thank you so much. Thanks to
EthicalGEO for inviting us. A quick word, before I start off some comments and some presentation for the attendees, on FPF and our background in working on all of this.

So, Future of Privacy Forum is a think-tank, we're based in Washington D.C., although now we have offices in Brussels and Seattle, Washington as well.

And we focus on the range of issues related to consumer privacy, specifically emerging technology and consumer privacy.

So, location data has been on our radar for many, many years since really the entirety of the organization's history, mostly from a consumer perspective, and especially as it relates to things like online marketing and advertising, which is at the crux of a lot of the issues I think we're going to be talking about today.

When the pandemic became the focus of our attention a few months ago, more than that now. I guess, location data was also at the heart of a lot of the commercial privacy issues that we were talking about with COVID-19, right, so FPF launched a series of privacy and pandemic workshops with global leaders to talk about these issues, and I was honored to be invited to participate in a paper hearing with the Senate Commerce Committee on commercial data privacy issues and unsurprisingly, all of the questions that we received were about location data, right? So this couldn't be more timely and important,
so, thank you. We're also pragmatists, I would say. We're not consumer privacy advocates like my friend, Jake at ACLU, nor are we a trade association. We try to find the center ground and the practical solution for emerging ethical and legal issues.

So all that aside, we can maybe dive into some of the basics. What I thought I'd do today and maybe we'll go ahead and move to the next slide.

What I thought I'd do with the next 7 minutes or so is just a little bit first about mobile location data, how it works. I think there's a lot of misconceptions here about what kind of data we're talking about it and who holds it, and how it's collected, so, I thought I would do some level setting that'll hopefully be helpful for the rest of the conversation, and then talk a little bit about the data flows, some of the potential safeguards and active safeguards that are out there, and some of the risks that are out there, and then maybe wind up talking a little bit about all of this in the context of COVID-19, and some of the contact tracing and exposure notification apps that we've seen around the world.

So first off, location data. There's so many misconceptions that we've seen out there. So, the first thing that's important to understand about location data is that we're usually talking about it in the context of a mobile device, usually your cell phone, but it's not limited to that.

as we move to an Internet of Things world, as we all start buying connected vehicles, and connected wearables, and everything else.
What we’re really talking about is connected devices and the signals that those connected devices emit and receive.

And this is, a little bit to me, at the heart of what makes this such a challenging legal issue too, when it comes to defining what location is and when other types of data become location data. So, in the context of the phone, which I think is the best place to start, some signals that the phone is receiving, have known locations.

So that's how GPS works for example. GPS satellites broadcast signals have known locations as they move through space. Cell towers broadcast IDs and cell towers have known locations, so you can use that to triangulate location. WiFi networks have been extensively mapped out through public and private efforts so that the reception of all of the different WiFi networks that are the neighbors, the coffee shop, the gym. Because we know their locations, you can infer from the signal strength of those networks, where devices are located. Other things like Bluetooth beacons, Bluetooth beacons are out there.
Other signals are unknown, or they're moving, right? So you're getting signals from moving devices, other people's vehicles, IoT, and the signals are not limited to GPS so, increasingly, we're talking about WiFi,

but mobile devices are also packed with other sensors. You can use microphones, you can use cameras, you can use near field barometers, magnetometers, all of these different hardware sensors to help infer more and more precise location.

So, next slide.

Let's see. This is the most common way that commercial entities receive location data sets and it's the focus and gets the most legal attention right now.

The role of the operating system on your phone, if you're using an iPhone, Apple, if you're using an Android, Google, right?

The role of the operating system is to interpret all of those ambient signals that we were talking about into a latitude and longitude.

And then that latitude and longitude along with usually other information is provided through an application programming interface to app developers.
or Horizon, and your other cell phone carriers. In fact, it's much more commonly available in commercial markets to get it from mobile apps through software development kits, and through the advertisements that are served in mobile apps.

So this is a little walk-through and we can come back to this if we want. But what we're looking at basically is an app developer that sends a request to the operating system and gets back a latitude-longitude measurement. It is possible in some cases, for the app developers to go around that process, you know, by looking out through Bluetooth access to see if they're beacons nearby, for example. But that's much less common. It violates terms of service usually, it would probably violate some legal regimes that we have here in the United States, but there are some technical workarounds. The most common use-cases, aside from providing the service of course, providing a ride-share alert or geofence alert, the most common use-cases tend to have to do with advertising.

So you can think of serving a localized advertisement, I want to send this advertisement only to people in Washington D.C. and therefore I'm willing to pay more for it. But you should also think about location data and advertising in terms of audience creation to do with, like, I'd like a list of people who go to coffee shops, people who go to the gym more, people who have been to this particular store, people who've been to my competitor's store, and also think about it in terms of measurement and attribution.
So increasingly what advertisers want to know is not just did you see the advertisement, but after you saw the advertisement, did you do something, did you go into the store? Did you go into the competitor's store? Did you do nothing, in which case that advertisement wasn't very useful? There are lots of other use cases too, right? So, it's obviously not just limited to advertising. We've got anti-fraud use-cases that are out there, a lot of analytics, political targeting becomes a major legal issue and there are a lot of use cases, beneficial use cases, I think, out there with State and Federal Departments of Transportation, related to urban planning, how are people moving around? How are they getting to work or commuting? Where do we need to build roads and sidewalks, and bike lanes? So, some of these issues, and Jake, I have a feeling we'll get into these later, but just to tee them up, some of the issues really involve whether people are aware of this kind of data collection. I think it's safe to say most people are not. Bundling of consent, so, when you give consent to an app, are you also giving consent that app's partners, or to onward transfers, and unexpected uses. So we've seen a lot in the news lately that some of this commercial location data ends up in the hands of federal law enforcement agencies for example, who are buying just the same way anyone else buys it because it's available out there in the commercial market. Okay, so I'm already like, going way over time. So I think maybe we'll leave some of the other slides for later Chris, if that works for you, and I'll just go to the next two.

So, again, this is just a quick overview of all of the different commercial entities that are out there. This doesn't even include government entities, right, so, because our focus is on the commercial space. Carriers are just, you know, in some sense, the tip of the iceberg. In another sense, they're also regulated more heavily.
So we saw a very large FCC find a couple of months ago related to location data that had been improperly shared and disclosed that originated with cell phone carriers. But it's really the apps, the app partners, the data brokers, the aggregators, any other third party out there, getting information from software development kits, and for mobile apps that are the bulk of the commercial location data sets out there, and I'll flag these. Entities are having to comply with generally applicable, so broadly applicable legal regimes. You've got the General Data Protection Regulations in the EU. If it's a global company, for instance, or if they've voluntarily committed to it, you've got the California Consumer Privacy Act now in effect with regulations, and most states have unfair, deceptive practices laws.
So, no location-specific laws in the commercial space exist to my knowledge yet. And we can talk about whether that's a good idea. But there are, at least there's some legal baselines that these companies have to comply with.

And it is a world, in the very bottom row here, of location analytics providers that are not working through the mobile app ecosystem. So what I think a lot of end-users and consumers aren't aware of, is that in addition to all of the data your phone is receiving and sending through mobile apps and through the operating system, just by virtue of it being a connected device, it's sending signals out into the world. Usually so that it can automatically connect to a network, right? So, when you get home, your phone automatically connects to the home WiFi, you don't have to do it manually because it's emitting signals on a regular basis that identify it.

So, hardware signals, including a Mac address, SSID information and that information, I would say, for a long time in the United States, wasn't necessarily considered personally identifiable within industry. That's rapidly changing,
and one of the reasons is that when those hardware identifiers remain the same over time, it's pretty straightforward to count and to track how devices are moving and devices are used as a proxy for individuals.

So, again, some of those use cases are benign. Most airports and stadiums are using this kind of ambient signal data from devices to track how many people are moving in and out of big spaces.

But it can get more privacy invasive when it's used to track repeat-visitor or to track where devices are moving over time, and none of that is subject to notice and choice, because it's not happening, there's no permissions layer, it's just signals that the device is giving out.

So, lots of different sources of commercial location data and maybe we'll wrap it there. Was that helpful because there's so much more we can get into? That's great.

well, you can reserve the right to bring up more of these if you need us to go back to the slides later. No, no, I really appreciate that though. Yeah, please. Why don't we stop on the resources page for just a moment. So I'll just flag, this is our website, you can find me on Twitter and FPF, and some of the graphics I was pulling from are from a recent infographic that we published for lawmakers on helping understand the world of geo location data., this is from a couple of months ago.

Yeah, and we should get into it more. I told you, we could talk about this all day. So it's good that we have so much time. No, that's great. No, I really appreciate that.

Yeah, you started talking about the kind of the risks and the safeguards, but unless you actually understand how all of this tech in your pocket works, you know, you can't understand the risks and you struggle with how to safeguard yourself, safeguard your family, your enterprise.
You know, I appreciate the fact that you talked about the electronic emanations outward, right? Because people are like, I clicked on the terms of service, you know, it's my choice, 148
00:21:57.055 --> 00:21:58.194
and at some point, 149
00:21:58.224 --> 00:21:58.404
you know, 150
00:21:58.404 --> 00:22:01.734
once you opt-in to owning a cell phone at all, any form 151
00:22:01.734 --> 00:22:02.694
of mobile device, 152
00:22:02.910 --> 00:22:05.095
you're on the grid and, 153
00:22:05.335 --> 00:22:05.724
you know, 154
00:22:05.845 --> 00:22:06.565
typically, 155
00:22:06.595 --> 00:22:12.625
unless you're a national security professional or like a prepper or 156
00:22:12.654 --> 00:22:13.045
you know, 157
00:22:13.045 --> 00:22:15.505
somebody who is really trying to prepare themselves, 158
00:22:15.505 --> 00:22:24.835
they don't necessarily know the extent to which they're exposed, and not really by choice other than the choice to participate in modern society with the cell phone, 159
00:22:24.835 --> 00:22:35.755
right? So, no, I think that's great and a great way to kick us off. So, now, I think we'll pass it over to Kevin, hand him the mic and get his perspectives on things, Kevin? 160
00:22:36.684 --> 00:22:50.424
Well, great. Well Chris, thank you. Thank you for giving me a chance to participate. and Stacey, thank you. I really enjoyed that perspective, and I found it very informative and I'm learning stuff everyday myself, in terms of just how this technology is evolving,
how it's being used, what the ecosystem looks like and I think to the point that you made earlier I mean, it's evolving so quickly that if you had this event six months from now, you'd probably have a couple of other slides you'd need to provide, both from a technology standpoint and a legal standpoint, right?

So it's really interesting and I agree, this is a really viable panel and discussion. From my standpoint, just to maybe add a little bit to what Chris said. I started out as a satellite imagery analyst before I went to law school, and so my background and interest, if you will, in location data is part of a larger interest around geospatial data in general, right?

Not just data collected from mobile devices, or some of the other technologies, but talking about drones and satellites, and all the other ways that location data is collected.

And that's important as I go through my remarks, because I think when we start looking at the legal perspectives on mobile location technology, it's important to realize that, as laws and policies develop around this particular use case, or this particular aspect of location, it could very well get caught up in the larger geospatial ecosystem and could have some significant impact on some of the things that people are trying to do,
not just here in the United States, but around the globe to deal with, not just COVID-19, but disaster-response and climate change, food security, issues that are also very much tied to location and require, or not require, better products and services can be developed if you have the granularity of the data, that issues that this technology can do. So I'll walk through that. That's sort of my overarching thought. And then I have, sort of, three major points. And then I'll sort of get down into the specifics and I apologize, I don't have slides on this, I'm just going to talk for a couple minutes, but when I first, sort of, thesis, if you will, is that if the United States had a comprehensive privacy, legal and policy framework, that balanced the risks and benefits of location technology, if that was in place prior to COVID-19, then contact tracing would have been more easily accepted, more easily implemented and, you know, hopefully would have had some significant impact on the pandemic in the United States. And as Chris knows, I've been sort of up there for a number of years, trying to sort of talk about these issues because we're seeing now the value of this technology, and as Stacey pointed out, the risks associated with it too.
So, I'm a big fan of the technology, but I understand, you know, because of my work, there's risk associated with it. But the time to do something is now so we can use the value of this technology going forward. I also believe that the geospatial community, and I'm not sure what percentage of the folks here are part of this. It's an EthicalGEO program so I assume it's larger than, sort of, the mobile technology community or the privacy community but there are a number of geospatial experts and professionals, geographers and GIS folks and everything involved. I think they know the benefits and the risks better than anyone else. They're doing this every day and a lot of folks that are getting involved in using location data have one or two particular use cases in mind, some of those are good, some of those bad, but the geospatial community has been thinking about this for a number of years. I often say that, you know, the geospatial community was big data before big data was cool. It's been understanding and dealing with these issues. But, historically, it's tended to look inwards in terms of who it interacts with and how working with solutions, and because of that is not as actively engaged in some of these discussions as I think it should be. Because, as Stacey pointed out, the laws and policies and regulations, they're being developed, and her organization and many others are participating in it, but you don't see many of the geospatial community doing that. And I think that's a challenge, because for some of the reasons I'll describe,
I think that location data and geospatial information in general are very challenging from a privacy standpoint.

Then the third point, and this sort of builds on the second is, I see a number, this is unfortunate from some of the work that I've been doing, and I see a number of presentations on how geospatial information, including mobile location technology can be used to really do some important applications around the globe, transnational issues, national security issues, you know, business issues, I mean the full gamut. As a lawyer, and looking at this, I always wonder, are you going to be able to do this four or five years from now? Are you going to be able to collect that information and do the things that you want with a law changing?

And I've said on several occasions, you know, I worry that you're going to have, sort of a HIPAA-type framework where it gets really hard to use because you've got to look at the definitions, you've got to look at the applications, you've got to figure out which of the groups you fit in part of, and if that's the case, you know, a lot of these applications may not develop or may not reach their full potential. And I think that would be a shame.
So I’ve mentioned before, and I’ll say it again, you know, location privacy, I believe is more challenging than privacy with other types of data. And I’m not saying it’s more important or more sensitive, and we could have that discussion, but, you know, healthcare data, financial data, there’s really sensitive types of information out there. But I think location data is more versatile and Stacey gave some examples of different things you can do with data. The example that I give is you can use location data with other types of geospatial information for a business to identify where it wants to put the store. The same information can be used by the local Department of Transportation to figure out where to build the roads to get to the store, so the people can get to the store. Consumers can use that to find the stores so they can buy, and robbers or criminals can go there to rob the store. It’s the same type of data, right? So, if you try to, it’s that versatility that’s really important. Also, there are just a number of different types of data that is location-enabled and that includes the mobile devices, and Stacey mentioned the IoT devices, and a bunch of other devices that are coming down but, you know, you can look at CCTV cameras that are location-enabled and have timestamps on them, they can be integrated into the sort of products and solutions and raised challenges, and we’re seeing that with ring, for instance. Drones are something that gets a lot of attention as well. That’s something that’s sort of come to the forefront over the past couple of years, but also satellites. People often say that satellites don’t have the quality yet to do facial recognition, and that’s true. But there’s a lat-long that can be geocoded, there’s a timestamp and there’s usually other information that can be used pretty, not without too much difficulty, to figure out what’s going on at a location, or who’s there or who was there if you aggregate it with other data.
So, even satellite data is going to do that,

is going to be an issue in the future, I believe, particularly as we move into small sat and if we have video type quality and pervasive satellites, I think it's going to be a really interesting issue in the next couple of years.

You start looking at key access cards, you start looking at credit card transactions, all of them are location-enabled and all contribute to both the solution and the issue. And that just goes to the point that I think this data is versatile.

It can be used in a lot of different ways and then we start looking at all the different sensors that are coming down on lights. You look at Thermal IR, you look at Lidar, you look at radar, the privacy issues around some of these technologies and Thermal IR is a real strong one, I mean, we're going to spend a number of years trying to figure out how to deal with that because there's some conflicting cases out there. There's going to be, trying to understand what the implications are.

So, again, it's not the mobile location data, but it is location-enabled, and it does, it is very valuable, particularly when you start using it with other types of location data and then you start looking at AI and machine learning. To do the processing you've got facial recognition technology. Again, all of those are issues in themselves,

but when you start putting the location stamp on them, or a location and a timestamp, they become increasingly more complex. And so, again, to go back to the point, the geospatial community is one of many that's dealing with some of these technologies, but the aspects of location really, I think, raise the issues associated with location more so than some of the others. I don't mean to downplay the others, and their importance,
I think, is there. One of the things that I think is interesting, and maybe it's not as big of a deal as I think it is for other people, but we have been giving away our location every time we go out, and we've been doing that for years. So, we go out into public place, we disclose that to people and we've gotten used to it. We go to a stadium and a mall people know we're there, right? And they know if we walk out with a bag, they know we bought something there. We're fundamentally changing that by putting concern around people's location, and I don't fully understand what that means. I mean, it has some implications around cases, like Carpenter, but understanding what that means and what the implications are going to be going forward and going back, I think are going to be really important because we never used to worry about it, and now we do and rightfully so, because other people are collecting it. But, how we deal with that, I think is going to be really, really interesting and is going to have some long-term implications about some of these technologies. To piggyback on that, I believe that the issues associated are more complex, I think location privacy is less consistent across the globe, and across communities. I think it depends partly on your age, your gender, your religion, whether you grow up in a big town or a small town. Everyone knew where I was, you know, the teachers knew where I was, everyone knew where everyone was, and what they were doing, because it was a small town. You didn't really have any expectation of privacy or anonymity. So just, an expectation,
I'm not saying it's right or wrong, but it's very different than for instance, financial information or medical records. You know, we sort of inherently don't want to disclose that, but now we're doing others, and I think that's a challenge from a regulatory standpoint.

I think location data is, from a privacy standpoint, incredibly powerful, and I think it was Joseph Jerome from the Center for Democracy and Technology, I think it was about six months ago, he put out a tweet that said that 80% of the privacy issues could be resolved if we get our hands around location privacy. Now, I'm paraphrasing a little bit there, but I think his point is that you have privacy issues, and then you put location on top of it and it gets to be, you have data and you put location on top of it, it gets to be a real issue, and that's because location is so powerful, you can tag other pieces of data to it, medical information, demographic information, statistics, social media. All of those things make location powerful. No matter how you collect it.

The more, the greater granularity, the greater consistency, the greater timeliness, the better, but you can get privacy issues without all that level of granularity or timeliness, and so, that's the challenge with location information. But on top of that, you know, there's so many different types of platforms that are collecting it and I ran through some of them; sensors, different sensors, different platforms. The user doesn't care, right? The user doesn't care where it came from. The user wants it to work. But if they have to start looking at what the platform is, because you've got different regulatory regimes around them that's going to be a challenge, right? So, if drones have certain data collection, mobile phones, the FTC has some, trying to aggregate those in ways that could be valuable,
whether it be for COVID-19, whether it be for a disaster, whether it be for a business application, it's going to be a real real challenge, and you're going to spend a whole lot of time with lawyers that you don't want to. I know some of these may sound trivial, but as a lawyer who, you know, drafts privacy policies, who drafts licensing agreements, tries to think through what the implications are, tries to apply them to the laws that exist today and where the law's going, it's really hard. It's very, very difficult and it's only going to get harder. And again, as someone who believes this technology can be really valuable, I worry about that because I do think it's going to have some restrictions, and some restrictions are good and are necessary for sure, but many of them are not, maybe there's a neutral way to figure it out, but that's a discussion that you need to have, informed technical people, operation people and legal people and regulators in the room to discuss, right? Just a couple of other points. The geospatial community is so large and complex that it makes some real challenges. So I include government, industry, universities, individuals, people of data providers and data collectors, both users and data collectors, both. I mean, it is an ecosystem. Often simultaneously, we're both collecting data, but we're giving our data away as well, and I don't mean that in a business way, but just we're sharing data back and forth. If you start to regulate that, you start to sort of say this group can't have it, or this group, we've got to be careful with, that ecosystem starts to shift a little bit because the data isn't available for others to use it, and maybe that's fine, maybe the risk is greater, but if you don't have the discussion about, okay, who's using it and how it's being used, and you just say that we're worried about this risk, you run the risk of not properly allocating the risks or understanding the risk in finding a solution that works best for everyone.
I think some of the other challenges are, it's much harder to find in my view, location
data in terms of what it is, is it where it's collected from, is it how timely it is?

Is it different you do by how large of an area it's collected, and you see in the in the legal
community and the regulatory community,
different topics,
different ways that people are trying to address it. At first, it wasn't addressed at all,
it'd be referenced, just, you looked at the laws, it would just say, location information or
geolocation information. Now, people are trying to define it, CCPA 2.0
has a definition, the Children's Online Privacy Protection Act has a definition, I think,
and there's a couple of other groups that are out there that I haven't had a chance to
look at, but it's evolving, but there's no common definition as to,
okay, if you collect data with this granularity, this frequency, this accuracy, then you've
got a privacy issue, or if you collect it from this device or this type of thing, it's very
much mixed.
And, you know, I tell people, as a lawyer, if the law's unclear, you don't understand the
technology, you don't understand how it's going to be used, you're going to say no
more often than yeah, than yes. That's how lawyers work, but that's just human nature.
Putting all those together I think it's going to be a really difficult regulatory, difficult to
regulate this in a way that balances the risks and the rewards,
It touches upon a lot of different legal areas, is inherently international and that raises a whole other spectrum of legal resumes you have to worry about. And so, I think it's important to sort of keep all that in mind when we go forward and we start talking about these issues.

Hey, Chris. That's it, I'm done. Thank you, Kevin.

I'm not sure if you just coined the term, or if it's old hat to you, but I've always heard of the expectation of privacy, but the notion that the expectation of location privacy is different, right? In different environments, because, you know, people know you're there.

It's a very interesting thing you put out there. I know, you know, you talked about, we've been giving away our location data for years, I know I have. But there was kind of that moment, I think my friend, Jeff, our friend, Jeff Jonas, he coined the term channel consolidation around location data, where, you know, I knew I was giving my information to those guys when I went there, and I knew I was giving my information to those guys when I used that toll road or whatever, but at some point it clicked and said, oh my God, you know, it's actually really easy for, kind of, anybody to throw all that stuff together.

Then that fundamentally made you, kind of, rethink how gracious you are handing out your location data to anyone, because it potentially went to everyone. So, anyways, I think you raised a ton of great issues. Before we go to a Q and A, we'll pass it over to Jacob now, to hear his perspective, and then I look forward to the Q and A with all of you.

Thanks. Thanks so much Chris. I really appreciate it.
It's great to be here and I appreciate the invitation very much from EthicalGEO, it’s a great program, and thanks a lot to Stacey and to Kevin for their fantastic and informative presentations.

I learned a lot and I think there's going to be just a ton of great material for the discussion, so really looking forward to that.

I would like to start off, maybe go to the next slide, by focusing on some of the risks of location information, just to kind of frame the rest of my remarks, and then some of the rest of our discussion. You can go to the next slide please.

And then, because we're talking about location privacy in the context of a global pandemic, I want to talk about two COVID-19-specific issues, contract tracing and population-wide movement tracking.

And those are areas where location data, I think could theoretically be useful, but as Kevin has gestured towards, there are complexities when you look at how that location data plays out in practice.

And then finally, I'll talk about some legal limits on the collection and use of location information.

There are a lot of legal limits under privacy law but I will focus primarily on our case with the ACLU challenging the Los Angeles Department of Transportation Selection.

micro-mobility location information, under the Fourth Amendment, the Constitution, and also some state's fashions.

So, if you move to the next slide please. So, when it comes to risks,

I think there's one kind of overarching concept that I
would love for everyone who attends this to take away. Next slide please.

And that's when engineers or lawyers, or potentially geographers look at data, it's very easy to think of it as something that is abstract, or that is disconnected from real people.

And I think that's especially true when the identities of the people the data corresponds to, are not apparent or easily accessible.

This is a sample of location information collected from micro-mobility sources in Louisiana, and you'll see that there's no names or addresses in this spreadsheet. It's very easy to look at rows of the spreadsheet and not have potential human cost involved. Go to the next slide. So, this is a picture of Fernando.

He was deported to Guatemala by the Trump administration, and separated from his daughter, Alison for almost two years. This is an image when they were reunited at Los Angeles International Airport in January 2020, after that separation. And we've all seen images like these,
and we have observed the human rights abuses that are taking place in our country when it comes to members of the immigrant community.

And I think we should all ask ourselves what enables those human rights abuses to take place. And there are, of course, many answers to that question, but one of them is location information, elected often in the first instance by companies, and eventually sold or produced somehow to the government.

Go to the next slide please. And this isn't hypothetical.

Last year in Northern California, the ACLU released the results of an investigation that showed that ICE is using automated license plate reader records to find and target immigrants for deportation. Next slide.

ICE is also buying location data from marketing companies, and those marketing companies get their data from apps that you might use to check the weather or find a gas station.

So it's not limited to military contractors who are providing this information to the government. These are consumer apps that we use everyday.

And so, the first question, I think we should all ask ourselves is do we need to be using detailed, identifiable location information at all?

Is there a way to achieve our goals, some of which, as Kevin points out, are really worthwhile and important. But is there a way to achieve those goals without use of location information.

Next slide please. So, in the context of our current pandemic, you know, we've all seen the event's hardship and the suffering that's caused by COVID-19, and as a result, there are new goals, new public policy goals, that really couldn't be more vital and important in this time. And some of those goals have been laid at the feet of technology and I'd like to start by talking about the contactors. Next slide.
So, actually, next slide, and then, the next one after that with the scientific article.

So, to me, the possibility of digital contact tracing was most clearly laid out in this really great article from Science from May of this year. And the basic idea is that when humans do contact tracing, there's a delay between when a person is diagnosed, and when other people who are potentially infected are notified, and that's where an app or something like that could be helpful.

The question is whether location information from whatever source might be helpful in making contact tracing, or as it's been more precisely called, exposure notification, more effective?

So, I'd just like to talk a little bit about that question. How effective is location information in enabling digital contactors. The next slide? Actually, could we just skip to like, three slides forward.

Yeah. That one. Thanks.

So, imagine we're trying to use location information to find out which of the contacts on this train, or in this workplace are potentially infectious. This is a diagram, by the way, from the Science article.

And we've all heard the guidance that six feet away for fifteen minutes is the threshold to be concerned about, and the ACLU released a white paper on this, and according to experts, the location information, like,
WiFi,

00:46:15.025 --> 00:46:15.414
location

00:46:15.414 --> 00:46:19.644
information or even QR codes associated with a particular place

00:46:19.644 --> 00:46:27.385
where people could go, is not sufficiently accurate and practice to accurately
distinguish between infectious and non-infections contact between two people.

00:46:28.045 --> 00:46:31.224
GPS data, from what we learned, comes closest,

00:46:31.500 --> 00:46:36.655
but even with a theoretical maximum of one meter for, sort of, modern cell phones,

00:46:36.925 --> 00:46:43.434
it's more like five meters to twenty meters in practice, when you're talking about the
strength,

00:46:43.465 --> 00:46:50.184
the visibility to the sky and how old the cell phone might be, and other kinds of
interference.

00:46:51.144 --> 00:47:01.885
And so, for location-based tools, like all of these, this, I think he demonstrates that
location information isn't likely to be very effective at enabling contactors.

00:47:02.454 --> 00:47:10.735
And that's why Bluetooth proximity information has been the technological solution
that has been offered, for example, by the Apple-Google framework that we've all heard
of.

00:47:12.864 --> 00:47:16.764
But even though the consensus among experts,

00:47:16.795 --> 00:47:31.465
and even from the technology companies building the contact tracing frameworks, is
that location information isn't likely to be useful, contact tracing apps are often seeking
location information from their users without a clear purpose for doing so.

00:47:31.465 --> 00:47:37.344
I hope at this point that you share my skepticism of those apps, as they seek people's
location information.
And, of course, you also have the problem that no matter what location information you use, people need to decide to install the app.

And in this paper it says that 50% to 70% of people need to install that in order for it to be effective.

And in my view, there’s a great deal of justified mistrust of the government, but also private industry, when it comes to collecting information.

And if people don’t trust that their information will be private, they won’t install the app, then that stands in the way of addressing the problem.

I think it’s worth putting that, adding that to our list of human costs that should be named. Past failures breed mistrust, and that mistrust undermines our collective ability to solve problems using technology in the future.

Next slide please. So, another place that we’ve heard location data might be useful is assessing how, kind of, on a population level people’s movements are changing,

in light of social distancing guidelines and some shelter-in-place orders, and that information is often called anonymized,

but in practice, it is anything but anonymized. Next slide.

So, The New York Times did this really fantastic piece demonstrating how people can be identified from, so called, anonymized location data. In January of this year,
Next slide. And this identifiable private data comes from consumer apps, or even telecom companies that in many cases, are just selling the information to the government.

Next slide. And when the government has immediate access to data that is pulled directly from apps, used by hundreds of millions of people. In my view, that's an end-run around the proper legal limits on government access to people's private information.

Next slide. So, and then, one more. Let's talk now about some of the legal limits. One more slide. Sorry about that. I'm just skipping a few here.

Let's talk about some of the legal limits that exists over people's location information and two laws I'd like to highlight specifically are the United States Constitution, the Fourth Amendment and the state's statute in California called the California Electronic Communications Privacy Act.

That's a law that is stronger than the federal Electronic Communications Privacy Act and there are also similar state statutes like CalECPA, as we call it, in New Mexico and Utah as well.

So, depending on where you live, you might recall that in 2017, many communities in the United States witnessed a, kind of, near overnight profusion of electric scooters on city sidewalks.

Those scooters offered a new mode of transportation for smartphone-equipped consumers, but they also resulted in complaints from members of the public and from city governments, over cluttered sidewalks, interference with right-of-ways and other complaints as well.

In Los Angeles, the Department of Transportation there, created something called the Mobility Data Specification, the
which automatically tracks the precise movements of every scooter rider on the street, and in order to get permits to operate in the city, all electric scooter and bike companies had to give the L.A. Department of Transportation access to that information. Next slide please.

And even more concerning is the fact that the MDS is planned to be a nationwide standard governing, not just micro-mobility like scooters and bikes, but ride shares like Uber and Lyft, and even flying autonomous vehicles and other modes of transportation as well.

So, in March of this year, along with the Co-counsel of the Electronic Frontier Foundation and Greenberg Glusker, we filed a lawsuit challenging the MDS and Fourth Amendment in a state statute CalECPA.

And CalECPA requires the government gets a warrant before they access location information, or other information about people held by service providers.

And given the importance of location information to privacy, as articulated in cases, like Carpenter, and also in CalECPA itself, this is a case that,
I think, really shows how government access to information is problematic and doesn’t and isn’t fully taking into account the legal limits that exist.

In addition to the purchase of location information, using permit processes, like LADoT is doing here, also represents an end-run around legal limits.

But in this case, they don’t, in my view, pass muster.

So, the solution here, in my view, is for government entities, and I think this applies to the private sector as well, to specify in advance, the policy goals that need to be achieved before collecting intensely private data about people.

And the approach we’ve seen here with respect to the L.A. Department of Transportation, and in other cities as well, is to collect all the information in a detailed identifiable form, and then figure out what to use it for after the facts. I would offer that that model has a pretty poor history when it comes to the private sector, and it’s not going to work out well for the government. I’ll stop there and thanks very much.

Wonderful. Thanks so much Jake. You know I think, and I appreciate this, kind of, swirl of issues where different parts of the government are trying to do different things, and their hearts might be in the right place but they’re, kind of, stomping on each other in ways that they probably didn’t anticipate until an ACLU lawsuit comes up at them and they’re like, okay, what are we going to do about that. But I was taken by your comment that, in the world of COVID-19, WiFi and GPS may be insufficient to actually determine contact, right? So if that’s the specific reason the app is being put out, and yet it determines that that goal can’t be met, then why are you doing it? And I think, you know, it came up in one of our international panels that the country of Norway has just decided that the efficacy met with the downside of the data breaches is sufficiently bad that they just scraped the whole thing. Now, that’s a small country, Norway, it’s probably like the small town that Kevin grew up in, you know, there’s other ways to go
about it, you may not need location tracking there, but it kind of makes me realize, you
know, this is a complex set of issues, so, thank you for that. And I think I'll just
roll into some questions. I do want to encourage all of you to feel free to not answer the
questions and answer a question of your own imagination,
because I think you guys have a lot of useful world views that would inform the
questions we should be asking. So, I'll start with these questions, but feel free to deviate
a bit from the program.
So, different nations are grappling with location privacy issues in their various COVID-19
contact tracing implementations in different ways. As American lawyers, or I'll say it this
way as American lawyers,
can you give us any simple models for how to think about how and why these other
countries are using and thinking about location privacy? Do you have any experience,
do you go well, of course it's going to work in that country because they think about it
this way and we don't think about it that way, or, you know, of course, it will work in that
country, it functions like a small town that Kevin grew up in?
Does anybody want to take a bite at maybe, maybe you're not international experts on
this stuff, but just things you've seen out there in the world? Stacey, you have a furred
brow, but I think that's because you have
an experience you want to relay. Well,
yeah. I don't know that I'll be much of an expert on the specific question you're asking.
Just help me with Canada? So, there are a couple of different ways to think about this.
There are countries that are adopting location-based models and countries that are
adopting proximity-based models.
There are also countries that are adopting centralized models versus decentralized
models and those two things don't always line up, right?
So, on a couple of the points that Jacob made. So first, whether or not location data has the effectiveness to properly do either contact tracing or exposure notification, I'm not sure that it's as ineffective as some of the earlier reports that we saw around cell-site location data, so, for instance, location data from cell towers, the kind of location data that your cell phone carrier holds already, and that governments started early on requesting access to. That kind of data is certainly not precise enough within that six foot level that you need for contact tracing and exposure notification. But app-based location data, if it's a phone that's requiring precise location data, and that person has Bluetooth and WiFi on, which most phones do, right? That data does tend to be very, very precise. The only thing that it might not give you is, you know, if you have two people within the same latitude-longitude, but there's a wall between them, you know, maybe that's not an exposure risk. But, other than that, I think you can get, sort of, the six feet parameter.
That's not to say that a lot of the commercial data sets that are out there are any good necessarily as they stand, because there's a lot of market incentive, particularly in the advertising space to use inaccurate data, because it doesn't really matter as much, for marketing use cases for example, that the data be really accurate and really precise. So, you see a lot of market puffery around companies that are like, yeah, it's super accurate and precise, and maybe the data really isn't. But designing an app from scratch, designing it in collaboration with private experts can provide really precise and accurate location data.

So I just don't want to discount it right away. I still don't think it's the right thing to necessarily be using because you have this immediate trade off of trust. People don't want to share their location data, right?

And if you can do it through other means, such as decentralized Bluetooth-based exposure notification, then you're going to get a much higher adoption rate.

I think some of the studies around whether you need 70% or 60% adoption rate, in order for an app to be effective, or been debunked a little bit. It's more like there is an increasing amount of effectiveness the more adoption that you have.

So, at low levels of adoption, you're going to have low levels of effectiveness, but maybe a little bit, right? And so, and then the more adoption, the more effective it's going to be.

So, collecting location data might work, it might work for things other than exposure notification like identifying hotspots.

And so a lot of public health authorities are interested in this for all of those other reasons, right? And then the counter is, you'll have much higher adoption rates for exposure notification apps that are based on Bluetooth.
The downside being, the public health authority doesn't have that information, it's not centralized, but the upside being maybe you'd save more lives because more people are adopting it and downloading it.

So, yeah, I agree with almost everything that Jacob and Kevin have been talking about. I think it's inevitable for those who are, sort of, in the audience thinking about this from a technical perspective.

The law is coming, it's inevitable that location data in my mind is going to be regulated, even more so than it's already regulated. There's regulation by law, regulation by code too. So, operating systems, regulating location data, more and more through things like Mac address randomization, changes to the advertising identifiers that developers can access, changes to the permissions, making them more and more granular, right?

So, regulation by law, regulation by code, regulation by social norms and the challenge, I think for lawyers is, as we see more and more political momentum towards greater consumer regulation in the space, the challenge for lawyers is going to be, how do you do it right? So, how do you write the definitions correctly, how do you write a location privacy law in a way that isn't underinclusive or overinclusive, and that's what we're focussing on. But it doesn't need to be updated in six months or a year from now, right, because of different technicalities or applications? Right, so I think the GDPR is a good model. I'm not sure it's being enforced as much as some advocates would like or how would envisage it being enforced, but I think the GDPR legal regime is a good model because it doesn't actually have any restriction for location data, the same as the GDPR doesn't have any restrictions around “facial recognition”, but those things are both heavily reciprocated because they fall under the category of personal information and it falls under the category of tracking people's private lives. So, similarly, I'm not sure we need a location privacy law in the United States, what we need is a baseline consumer comprehensive law that established protections for personal information, whether it's collected through your mega drive sorts, or an app developer, or through facial recognition, or whatever the method is of tracking people in their personal lives and using that information for unexpected purposes, that should be regulated. And that's, yeah, exactly
Kevin, that’s how you keep it from having to be updated every six months, even though updates probably will be needed over time through things like rule making. Anyway, just some stuff off the cuff. Yeah, great. Thanks for starting us off Stacey. Kevin, go ahead.

Yeah, so I have talked on this issue in a number of international settings and I think a couple of things that impact this issue is one, as I talked about in my remarks, I mean, different countries, different cultures have a different sense of location privacy than others, right? So on some, it’s a much higher concern, in some it's much lower. And some are concerned that they don't want the government to have it. And some are concerned that they don't want industry to have it, right? So, there's this cultural aspect to it. And then to Stacey's point, there are parts of the world, and Europe being one, that have an overarching privacy law, that, at least at a very general level, covers some of this. So, you can, one, you've got a whole bunch of people who are educated in this, and are thinking about this both lawyers, operational, technical folks. But also, people who are, you know, you've got an enforcement mechanism if someone goes to far. And, you know, it's not perfect, clearly, but there is that there and we don't, you know, the United States doesn't have that and it has a lot of different, it has a sense of, as we're finding out, a sense of individualism that adds to the complexity. So I do think we have some unique challenges here, which is why we are where we are, right? For good or for bad, right?

Jacob. Thanks, Kevin.
Good. Yeah, it's such an interesting issue, and I think the, I'd like to pick up on one theme in both Stacey's and Kevin's remarks, which is this notion that there's cultural differences with respect to location privacy.

And, you know, I think we talk about this in terms of comparing the United States with other countries, or other continents.

But, you know, the United States is not a model and they are going to be deep cultural differences in the United States.

And, you know, with respect, specifically to something like contract tracing, I think, one of the reasons that I laid out with respect to the risks to immigrant communities, or the experience that Black people have with police violence and over-policing in their communities, those are going to give rise to different levels of willingness to share information from those communities, and I think with very good reason.

And that has implications both for the sort of ethicacy of contact tracing as a general matter,
for the equity of contact tracing.

If white people in the United States, on this panel we're all,
it appears, white people.

We don't necessarily have the experience of being concerned about our communities, our families, ourselves,

our bodies being harmed

as a result of information about us being held by law enforcement. And that,

I think, means that something like contact tracing could benefit white people or people without that history of over-policing, but would not benefit Black and Brown communities,

and that's something that I think needs to be a really just sort of explicit part of the conversation.

And I think that, kind of, leads into the notion that that has to be taken into consideration with respect to manual contact tracing as well.

And we're just talking about people.

One

detail about this from a recent discussion that they've had in the California legislature.
considered a few contact tracing-specific privacy bills.

And one of the provisions that, at the beginning, was in those privacy bills, they said that contact tracing information that was collected cannot be used by law enforcement.

And the reason for that, I think, was that some people might think that if law enforcement had access to information about them, they’d be targeted by law enforcement, their communities could be subject to further policing, and that would put them in danger. And so they wouldn’t consent to the contact tracing. And the fact is that government interest, law enforcement interest, pushed back on it.

that’s an indication that we do have a, kind of, deep, substantive difference of opinion with respect to whether or not certain kinds of things that should adhere to the public benefit, also can be used by the government to harm you.

And I think that’s a difficult conversation to have, but a vital one. No, I think that’s a great point. I mean, the cultural references all of you are mentioning. But we have, as we’ve been putting together these panels, we’ve had a lot of interaction with international colleagues, and, you know, like, we talked with our friends in Taiwan and, you know, they framed all of this COVID-19 as another natural disaster
the same way a tsunami or a typhoon, or anything else is a natural disaster. And there
was a kind of cultural comfort with the government, knowing where everybody was
because it's the government that's going to send the alert that says,

01:08:39.720 --> 01:08:50.994
'a tsunami is coming, run from the beach', and in the same case, they were sending out
alerts saying, 'there's too many people in this public park, you couldn't possibly be, you
know, socially distanced enough'.

01:08:51.295 --> 01:08:58.045
But, you know, there aren't the same social divisions, or at least they don't appear to be.
I'm sure there are that

01:08:58.045 --> 01:09:12.564
I'm unaware of, but there doesn't appear to be the same social divisions as if they went
into a Black neighborhood and started slicing the data and handing it out to law
enforcement around enforcement. So, I appreciate those comments for sure.

01:09:12.810 --> 01:09:18.414
Does anybody else want to chime in on this topic before I move back into some other
questions? I see two hot mics.

01:09:20.244 --> 01:09:30.175
No? Okay. So, thank you for that. That was a great discussion. To talk a little more on the
international side, I guess I call it more transnational.

01:09:30.324 --> 01:09:31.104
So now,

01:09:31.104 --> 01:09:31.914
with all of the COVID-19

01:09:31.914 --> 01:09:34.765
related travel bans that we

01:09:34.765 --> 01:09:36.145
as Americans are subject to,

01:09:36.145 --> 01:09:50.965
but so are many others, it's hard imagining the world reopening to international travel
without some sort of, I think the term is health passporthing. Given the international
travel between different sovereign nations is more of a privilege than a

01:09:50.965 --> 01:09:51.895
right, I mean,
I guess a citizen has a right to go home maybe,
but the rest of us don't have a right to enter somebody else's country.
All of us will have to disclose much more about our previous travel and health status.
What location privacy issues will this force us to deal with?
And I'm sure all of you have thought about, you know, this mobile location tech. When I just move from America to Canada on a regular day, right? I'm changing jurisdictions, there's changing issues.
Maybe, how should we think about this, as we clearly are going to wade into some kind of health passporting? Kevin, your mic's hot. I don't know if that means you're volunteering.
No, I just, it's easier for me to have it on because I couldn't operate it with my mouse, but that's fine.
because they were potentially exposed to a COVID-19 issue then you’d not let them in

because they were potentially,

when in an area where there was polio,

or where there was something else,

right? But that's a higher level policy issue. But we do it for foot and mouth, right? Have you visited a farm? No, no.

But, yeah, I mean, there are things. It's a complex issue and a lot of it doesn't have to do with location.

I do think and I think this is going on now and probably was better than I but,

you know,

I wonder if you stop it, if you have to turn your phone in as you enter the United States and they have the ability to find out where you've been with,

enter the United States and they have the ability to find out where you've been with,

where you've traveled,

why have you gone there?

Who'd you meet with? I mean, that's going on now, right? And having traveled and been to places that probably, I've been worried that they're going to do that. And, you know, in some ways you sort of prepare for that, right?

In terms of what device you take or what you disclose. But I do think that's going to be part of where we move to, right? I mea, people are going to be like, where have you been, who have you been with? There's going to be a database
that's going to be able to tell what activities were taken on there and, you know, hopefully, it's a privilege for sure, but it's certainly one a lot of people have taken advantage of over the past ten years or so. And I would argue that it's made the world a better place, not a worse place.

And I would hate to see, again, because of the trade off between balance and benefits and risks, you know, certain sites saying, the risks are to great, we can't let him or her in, because they went to someplace A. Particularly, and you mentioned this earlier, you know, the data quality issues, you know, the ability of the, you know, if we look, we're using artificial intelligence and machine learning to make those decisions. I mean,

there's a lot of potential issues, which, you know, everyone on this call probably is aware of, but I do see some countries implementing that. Some are doing it within their own countries, right? Right. Passports, but they're doing it in their own country. So I do think it's something we'll need to worry about in the future.

Great. Jacob, I see your mic. So, Kevin, it's a great issue, just to spot and I can talk a little bit about device search at the border, and I think it'll be really interesting to see how this issue of device searches at the border plays out when the potential risk of people coming in from other countries where there are elevated coronavirus cases, although, right now, wherever they come from is going to be better than here. So there's that. So, and I’m summarizing this law based on memory, so no promises on correct.

So, when somebody comes to the United States, there is an ability for the government to search their belongings, and that includes their devices to some extent.
or what they call, or a non-forensic search,
and that's just whether something is plugged into the device and information is extracted off of it,
that would constitute a forensic search. And in the night circuit right now, you actually need a reasonable suspicion to my recollection,
to do a forensic search, and I think that's what you would need in order to rigorously assess whether or not somebody has been in a place where there was heightened coronavirus risk.
And so,
I think that reasonable suspicion is the thing that I think is going to be questioned when it comes to assessing whether or not this kind of search is permissible under the law when it comes to looking at people coming into the country and thinking about coronavirus as a potential risk. I think it's a fascinating area,
and it's going to be an interesting thing to watch as the law develops.
Yeah. Great. Stacey, did you want to chime in on this one at all? Yeah, it's a tricky set of issues, right? I think the jury is still out on immunity passports just with the science not there yet on whether we can actually establish that kind of thing.
I think there are issues with scale. It takes a long time to roll out these sorts of things. And by the time that there was an effective system in place, the whole question might be moved. The thing that would be, I think, arguably, easier is what Jacob's describing? So travel restrictions based on detailed location history and

I haven't seen that at a sort of technical level of searching a phone, to determine the location history and I think it would raise a lot of concerns, right? So, it's challenging to distinguish between that use case and a use case involving, checking anyone who comes in at a border for suspicious-looking location histories, right? So, the question is always about balance.

Can you achieve the same goals through less invasive means? And if so, that's certainly going to be the right answer. Great. Jacob, did you want to chime back in? I want to make one point about immunity passports. I completely agree with Stacey that there's just the sort of, like, technical issues to whether it's possible to do that. But I think there's also the question and incentive.

I mean, you know, we don't want people to be taking the risk and infecting themselves in order to get a job or to be able to travel. And, you know, the epidemiological and also the disease characteristics of COVID-19, I think are kind of really, really problematic or complicate this and make it very difficult. Because, you know, a lot of people are asymptomatic when they get COVID-19. Obviously, like, older people are more at risk.

And so we really wouldn't want to put a regime in place, either a practical regime or a legal regime that encourages people, maybe younger people, to infect themselves, recover and then be able to get an immunity passport so that they can get a job in the midst of the economic crisis.
And, you know, of course, those incentives are going to be felt most acutely by people who have lost their jobs, or who are economically struggling.

And so, you know, we've already seen vulnerable communities already experiencing the harm of COVID-19 disproportionally. And I have serious concerns that any health passport would make that worse. Great. So, I've got another question, it's international-transnational in nature, I'm always struck, you know, when I land in another country, open up my phone, I get that text that tells me what my data rates are going to cost and things like that, which I assume, I don't know if that's just my carrier or if it's a legal thing, but, you know, we don't have a similar thing for location tech, kind of, location privacy policy. Given the transnational nature of location tech and data, and the national and even sub-national nature of location privacy law, how do you think of the responsibility of public sector jurisdictions and even private sector service providers to informing users, consumers, citizens, of their rights and the risks as they move around the world? Like, should I get the text when I land that says, here's the summary of our location law by the way, here's the agency that tracks you, or, you know, it's illegal for anyone to track you by the way. How should that work or how might that work in the future?

Ah Kevin? There you go. It's like a game show, who hit the buzzer first. Go ahead Kevin.

So I'm going to answer a little bit differently, I think, although I think it's in the same realm. Okay.

I think it's really hard because of the nature of location information to come up with a one-size-fit-all privacy policy,
it’s the Wild, Wild West here, everyone’s collecting your location. Good luck. I mean, unless it’s something that simple or something like that, I just think it's really hard. And that goes back to the discussion.  
I had about, you know, why this is so different because of that right? And so that’s my only point.

Does anyone else want to pick up on that? I mean, I agree. It’s complicated. That's kind of why I put the question out there.  

Jacob? Yeah, so I think it would be remiss not to talk a little bit about the assurance to decision and response to this question.  

just recently  
the EU’s highest court issued a decision invalidating a data transfer agreement between the European Union and the United States known as the Privacy Shield.  

And the privacy shield,  
just generally speaking allowed companies to transfer data and not be out of compliance with the GDPR.  

But,  
in this case, the EU Court of Justice said that because of national surveillance law in the United States,
and because of the ability for the government in the United States to access communications that enter the United States, that Privacy Shield was invalid.

And so, you know, there's a lot of concern that the fact that the federal government in the United States has access to the private communications and even just the data flows that are happening within companies in the cloud, for example, could be put in question by, by the GDPR because they can't take advantage of the Privacy Shield anymore.

And so, your question was about what sort of public sector responsibility is and, you know, there, I think there's a difficult discussion to be had between the private sector companies and also the government about how the United States government's access to private information is actually really standing in the way of effective and efficient transfers of data by businesses.

And, you know, this, to me, is sort of, the chicken's coming home to the roost, by the surveillance state, but I think that's something that should be part of the conversation as well. Yeah, great. You anticipated my next question, but I'm going to ask it anyways. Stacey?
Did you want to chime in at all?

It's a really good point. I think it highlights the main challenges with having that kind of notification, even if you wanted one because it's really, sometimes it's less about the geographic location that you're in, and more about who's holding the data, who's getting the data, which is usually across state and international lines, right?

Yeah, it could be physically located in the United States using ads that collect location data and sending it to another country or another state. An app from a European country that's reselling the data to an American government? Yeah.

Chris, can I take a question? Yeah, please do. About Schrems II,

I mean arguably there are European countries that have significant access to personal information as well, or can get personal information as well,

but they are subject to GDPR,

so,

it's not,

you know,

you don't have to worry about external transfers,

right? So is the issue as much about, you know, the U.S. government's access, or that we don't have a federal privacy policy in place that would deal with some of these issues?
588
01:23:44.279 --> 01:23:55.435
Well, so, I mean, in reading the European Court of Justice’s decision, I mean, I thought that the main focus of that analysis was the U.S.
589
01:23:55.435 --> 01:24:06.744
government access to information helping the United States. I think it’s possible that a federal privacy law might do something to ameliorate those concerns.
590
01:24:06.744 --> 01:24:10.585
But I don’t see how you can not,
591
01:24:11.550 --> 01:24:24.534
how you can get to a different result, if you look at the Schrems II decision without having, you know, reform of some of the surveillance laws that emanate the concerns of the European Court of Justice.
592
01:24:24.715 --> 01:24:31.074
I say that, being an interloper in transnational data flows and the GDPR,
593
01:24:31.074 --> 01:24:42.265
so defer to others expertise there, but reading the decision, it does seem like the surveillance law was the main concern, and that you can’t get around it without reform there.
594
01:24:43.439 --> 01:24:47.005
Okay. Anybody else want to chime in on that?
595
01:24:48.180 --> 01:24:58.944
So, okay. This has come up at least twice, but I want to ask it in a pointed way and see if it changes the answers or if it gets us to a solution.
596
01:24:58.944 --> 01:25:11.814
So, for a long time, privacy discussions have been about a citizen’s rights, more recently a lot of new privacy laws have focussed on consumer rights, companies and their use of your data. With governments
597
01:25:11.814 --> 01:25:24.805
increasingly purchasing and consuming mobile location telemetry data, collected by commercial platforms, we now face a complicated collision between these two worlds. How do you see this
598
01:25:24.805 --> 01:25:29.244
shaking out over the next arbitrary time horizon?
599
01:25:37.314 --> 01:25:50.604
I'm going to give it to Jacob. It was a close one. So, I mean, I think the short answer is not well.

But to give us kind of a hint of what I think is a regulatory framework that I think would make sense. I like to highlight some of the work that the ACLU of Northern California has done, and also the ACLU of Massachusetts has done surrounding facial recognition.

So, I think it's a huge concern that governments are now buying information from the corporate sector and using that information as essentially a replacement for what would've required a process in the past.

And I think it's a difficult issue, and that acquisition has fairly few limits in terms of actual legal prohibitions.

The sort of good news is that in many cases, the federal government, and also state governments have sunshine laws that actually gives people access to the facts of that information, that those contracts exist and that information is being collected in something about what information is actually being searched, and that's how we got access to the fact that ICE was purchasing automated license plate reader data, and using it to find immigrants and deport them. So, sunshine laws are a big part of the response.

So, for facial recognition, our team has works on bands of facial recognition, used by government in San Francisco, in Berkeley and then ACLU of Massachusetts has done it in Boston and Cambridge and Brookline, and those plans, generally speaking, include a prohibition on acquisition of services,
or acquisition of data from private entities that are doing the special recognition themselves. And so, I think that's something that needs to be thought about in privacy laws, whether it's privacy laws for government conduct or for also, private industry, is thinking about really problematic and harmful acquisitions for data, and then putting in place prohibitions where it's appropriate.

Great. Does anybody else want to pick up on that? So, it's a couple of different things that I think Jacob raised, right? One is, the government's purchasing location data and other types of data as an end on getting a warrant based on probable cause approved by a judge, right? That seems to clearly be a violation. I think there's a lot of consensus.

We could introduce a law that I think would get a lot of support and possibly there will be one coming up in the next few months that would cut off that kind of access, but local governments, in particular, and you see this with a lot of the smart city efforts are interested in acquiring data for other purposes. They have, I think, a healthy skepticism of tech companies who want to run these things for them, and they typically commit budgets, right? But they're interested in using data for the same reasons, for the same sort of good beneficial reasons as anyone else, is any of the smart city tech companies, which involve things like improving urban planning, improving transportation.
The problem, I think, is, they typically don't have the data governance laws, norms, establish standards, resources as private companies.

So they want to get into the data game, so to speak, but don't have the right data governance restrictions.

And so that data ends up getting collected for one purpose and then potentially reused, or sort of sent across the hallway to a law enforcement agency.

And then there's law enforcement agencies, or other agencies, Departments of Transportation, for instance, that are interested in purchasing data, rather than collecting it directly, like DoT, but just purchasing the data for their own sorts of analysis.

And when the data is out there and commercially available in commercial markets widely,

understandably think that it's a strange outcome for it to be widely commercially available,

but not available for a government or non-law enforcement non-immigration, right?

non-enforcement purposes. So, yeah, we're absolutely seeing this direct collision of public and private concerns, and public and private legal regimes that's going to be really challenging to sort out, right?

So we've been in support of a fine consumer privacy law for a long time. I think a lot of people don't realize that the 1974 Privacy Act originally applied to the private sector and public sector, and then got limited and now only applies to the public sector.
Other regimes don't do that. So, the GDPR, for instance, applies to both public and private entities, and we can take an approach in the United States, but we have such a complicated technical regime already in place that just the political momentum is challenging.

But that's probably ultimately where it needs to turn out. That's fascinating. I did not know that that was how it started in 1970 and then it bifurcated from there. That's interesting.

You know, we've got a couple. The GDPR? I mean, yeah, before, I mean, you can make a really solid argument that the GDPR is based on the 1974 Privacy Act, certainly based on the FIPPs, right?

Even though we're, sort of, looking to the EU as being this gold standard right now, all of the fair information privacy practices in the United States, and of United States origin to both privacy and data protection and we're kind of, in a lot of ways, forty years, fifty years later, coming back to our roots.

They've been eroded as it relates to private sector data collection. You know, it's interesting, you know, we've had some other folks on previous panels. We had Jeanne Holm from L.A.,

their Chief Data Officer, but also Kate Garman from Cityfi, and, you know, Kate talked quite a bit about the surveillance, or, I don't know, not really anti-surveillance acts that she helped put in place
in, I want to say, Seattle, and also some work, maybe in Kansas City,
where,
you know,
you know,
looking at
which individual pieces of technology and data will we allow and for what purposes and a new one isn't allowed to be deployed until it's gone through an entire process where they look at social impact and whatever and,

it may be an onerous process,
but it's a deliberate process with, kind of, clear open use. And as somebody that's deployed a lot of technology into,

it doesn't actually happen as fast as you think it does anyways, that process.

may not actually slow anything down, but, you know, I mentioned it a little bit in those surveillance laws at the city level because it, you know, Jacob, you brought up facial recognition and that's happening at the city level, and
Kevin's brought up all these Internet of Things, and Stacey's worked all this smart city tech, you know, we talk about, not federal regulation, but what role does state and local, putting together in our jurisdiction,

here is what's allowable, what's not allowable. Here's what is disclosed. Here's what's knowable, every citizen can know what, you know, what we're doing, etc, in terms of, you know, what might broadly be rolled into surveillance, because that impacts COVID-19,

right? We're rolling things out for COVID-19 surveillance,

but then when COVID-19's done, do we just leave that there? Do we sunset it? How should we think about this stuff at a state and local level, given some of the precedents that have been set with surveillance laws? Jacob, you opened your mouth. Yeah, that's right.

So, thanks for noticing.

Yeah,

so I think the state level and local level surveillance laws like this are really critical. In the facial recognition bands that have been put in place in San Francisco, and Oakland, and Berkley, are actually,
or are on top of existing surveillance rules, like the ones that you described in Seattle and in Kansas City.

And, just generally speaking, those laws, and it's called community control over police surveillance, and ACLU has a page about it, we have a model, a model city ordinance, and a whole bunch of information about all the different places where ordinances like that have been passed. A basic idea to bring some democratic accountability to the acquisition of surveillance technology.

And so, to be super clear, like, if a city wants to buy a drone and, you know, take a whole bunch of pictures of really granular pictures of people's movements. Under the surveillance ordinances, they could do that. They just have to have a proposal, they have to have a use-policy, they have to have, you know, a city council meeting or something along those lines, where they give people the opportunity to comment. And then they have to have trainings,
and then they have to have annual assessments to determine whether or not the rules are being followed and to have, kind of, ongoing accountability within the community with respect to the use of that technology.

01:35:20.454 --> 01:35:33.954
I think that's, kind of, a model that I think is effective for the kind of surveillance technology that maybe isn't as problematic as something like facial recognition.

01:35:33.954 --> 01:35:48.145
And so, I think that there's a pragmatic distinction being drawn, for example, in places like San Francisco, looking at surveillance technology as a general category, in saying cities can buy it, but there needs to be democratic accountability and oversight and transparency. And then facial recognition, which is such a kind of problematic, dangerous, toxic technology that the city can't purchase it at all,

01:36:01.645 --> 01:36:08.125
and sort of saying, for some things, there should be a ban, for most things, there should be democratic accountability and transparency.

01:36:13.225 --> 01:36:17.274
Stacey, you have some experience in this. What are your thoughts?

01:36:22.104 --> 01:36:26.635
The question is around the role that local cities and local city regulations claim, right?

01:36:28.284 --> 01:36:39.175
Yeah, I mean, a huge role, right? Because nothing's happening at the federal level. Ideally we need a federal baseline for at least the commercial side of this.

01:36:40.795 --> 01:36:50.215
And I think there's a good argument that that necessarily has to preempt some of the city level ordinances and some of the state level laws,

01:36:50.694 --> 01:36:56.664
but not all are clearly some issues that are inherently local in my mind.

01:36:57.715 --> 01:37:02.725
But if you end up with different private sector regulation,

01:37:03.564 --> 01:37:04.524
in different places,

01:37:04.524 --> 01:37:06.805
as you go state to state and city to city,
if you're a company that operates
in all of those places,
you end up,
not being able to build an internal compliance regime, right?
To be able to comply with all of those laws. Bans are a little bit different, right? Because
a moratorium or a total ban on the use of the technology in a particular geographic
area is pretty straightforward, right?
Just don't do that thing. Where it becomes challenging is when you have different
regulations around things,
like,
whether people need to consent or whether they,
it's okay for them to just be able to opt-out or what kind of access to information do you
have to provide to the residents of this city versus the residence of that city,
versus the residents of this state.
We're, sort of, at the very beginning of that. There really isn't very much regulation out there. You can, kind of, count it on maybe one or two hands, but as things progress over
the next five years, it'll be really important to have
at least a baseline of a uniform set of both rights and obligations for companies.
Chris, can I just go into a couple of points? Please.
01:38:21.595 --> 01:38:25.135
Understanding the risk, I worry that the,
712
I worry that
713
01:38:28.734 --> 01:38:40.494
a balkanized, legal, regulatory framework on these technologies by city, by state is
going to make
714
01:38:40.914 --> 01:38:43.284
the ability to do some of the things,
715
01:38:43.645 --> 01:38:43.885
you know,
716
01:38:43.885 --> 01:38:50.185
that the geospatial community more broadly wants to do, or even within communities.
717
01:38:50.185 --> 01:38:50.454
I mean,
718
01:38:50.484 --> 01:38:54.055
a lot of larger issues involve data from,
719
01:38:54.564 --> 01:38:54.805
you know,
720
01:38:54.805 --> 01:39:01.585
across the state or across all urban communities or across different communities and
yeah,
721
01:39:01.585 --> 01:39:13.284
it requires data, and increasingly it requires data with more granularity. And if you've
got these, to Stacey's point, if you've got a ban, then you don't have it.
722
If you've got to try to figure out consent and notification requirements to go through
public policy, you know, public forms on these things. I think it gets really difficult. And
I'm not saying that there aren't risks associated with this, there's risks associated with
all of them.
723
But it seems to me it's harder at the local level in particular, to have a meaningful
discussion around the risks and rewards a federal and international level.
724
And that's partly because of just the way local politics works, is also partly because just what their particular interest is.

So, I just throw that out there. I think both Stacey and Jacob are right,

I mean, that's the way we're going, because we don't have, you know, whether it be dysfunction in Washington, or whether it just be, we're not adult enough yet to have this discussion.

But that's where we're going and I worry if it isn't fixed sooner, rather than later what that's going mean for a lot of types of geolocation and geospatial information. Great.

Yeah, just so. Ah, you're fighting for the mic. This is great. I'm going to go to Stacey, then Jacob. Go ahead, Stacey.

I agree with that. I want to add the added wrinkle that a lot of private sector companies that are dealing with location data sets are for purposes of their own risk minimization, keeping it as anonymous as possible.

It's clear that that data is not anonymous in most cases. I mean, Jacob, you've made a really compelling point, I think the evidence is clear on this, right?

Once you have a persistent identifier following someone around,

you can

re-identify them fairly easily,

given enough time and precision.

But companies,

most of the commercial location
intelligence firms are not tying it to name, they're not tying it to any other ID, they're doing their best to try to keep it as anonymized as they can.

So, the challenge that that creates for different privacy regimes with different access and choice requirements, is that, sometimes, in order to comply with those, you end up making people re-identify their own data, when they otherwise wouldn't.

So, if, for instance, you have a practice of redacting, dwell time overnight, which shows you where a person lives, or you redact sensitive locations, like schools and churches and things like that. And then you are faced with a local law that says this data is personal information, how do you respond to that? How do you know whether the data you hold is a resident of the state, somebody passing through, or in some way triggers your legal obligations without taking additional steps to figure that out. So it's challenging. Jacob, you wanted to chime in? Yeah, I think there's a really interesting discussion to be had about, kind of, what the right level of, I, sort of, as a policy matter, where we want policy innovation to happen and how that balances against, so putting pretty protections in place that protect people today versus waiting, and, you know,
well,

the larger you get, as you get from the local, to the county, into the state, to the national level,

the political lift in order to pass a law

there is heavier and heavier and heavier. And I think probably, at the national level, the political lift in the recent past, and the immediate future is infinite, right?

Like, there's no possibility that would happen. And given that,

I think that we all need to be thinking about the fact that putting in place laws that protect people is kind of, like, is necessary and, you know, that we should, as a result, expect

and accept some balkanization of the regulatory environment for companies as a result of the fact that the national government isn't likely to act on a lot of these issues.

Even state governments are unlikely to act, I think for similar reasons, relating to corporate influence, over state legislatures. And so increasingly, the place where policy making can happen, and I think it's actually quite sophisticated,

thoughtful policy making, is the local level.

So, I don't disagree with anything that you've said. I would say, though, that at a local level,

my guess is that people, there are technologies and applications for data, particularly on that, and putting aside industry, just on the government side. There are things that civil servants could do with data

that would make transportation better, that would make the streets safer, that would make smart cities better. I mean, good, good useful uses,
right? But if they're prohibited to do so because there was a very, you know, for whatever reason, something bad happened or someone gets concerned, they don't have the big budgets,

they don't have, they often don't have people who are out there pushing for them and those are the people that's going to get hurt, and I think that's probably happening, and so I understand what you're saying, and you're right,

it's partly, as Stacey has said, a number of times, we need something at a national level to sort of have those discussions and to think those through and give everyone an opportunity to play.

But at the local level, I don't think those discussions are taking place with the same level of vigor and education and understanding. That's my sense.

I also agree with that,

there are some things I think, which might be prohibited at the local level,

but I also don't want to discount the things that are possible at the local level without using,
And just to sort of, like, lay out a few of those, because I think it's worth being specific. With respect to micro-mobility, like scooters and bikes, there's a huge important policy goal, and making sure that those modes of transportation are available equitably across the city and not that scooters and bikes are just located in rich neighborhoods and not in poor neighborhoods because those represent in some instances a low cost, a lower cost way of getting to work, for example, that those communities might not otherwise have. There's also a really important goal of making sure that public rights of way are free from obstruction, to make sure that disabled people can use sidewalks and crosswalks and such, and that those aren't interfered with by scooters and bikes. And then there's of course the, something that's been mentioned a few times,
which is where you put roads,  
01:46:15.685 --> 01:46:18.024
where do you put bypasses, and things like that?  
Where do you put stores? All of those goals, I think can be achieved without having highly granular maximum precision location data about individual trips.  
01:46:32.125 --> 01:46:33.024
If you’re building a bike path,  
01:46:33.024 --> 01:46:33.534
for example,  
01:46:33.534 --> 01:46:48.414
you can aggregate a whole bunch of trips together and not have any individual be identifiable and you can do a pretty robust aggregation, and you can still find out where populations are moving and you’re not identifying people. With respect to  
01:46:48.414 --> 01:47:02.154
things like disability, or with respect to equitable distribution of micro-mobility, that can be done without knowing anything about any individual trip, but just where scooters are left when no person is on them.  
01:47:02.670 --> 01:47:15.265
And so, I think that the solution here is to think about the goal at the outset, and then design a process, including access to information, which minimizes the privacy harms.  
01:47:15.324 --> 01:47:27.715
And I think a lot of public policy goals are possible if you do that. It does take more thought and more time, but I think you can get both the sort of praise-worthy policy goals and also the privacy,  
01:47:28.465 --> 01:47:41.935
if you do the process right. That was a great discussion back and forth. I don’t want to cut it off. Does anybody else want to chime in on that? No, I totally agree with everything  
01:47:41.935 --> 01:47:45.505
Jacob just said. I’m interested in, sort of, the challenge  
01:47:45.505 --> 01:47:49.614
when you have multiple different private companies that are all, sort of, collecting similar data.
I think what you can use aggregate information, you can use more limited types of information to serve the policy goals without requiring that those companies transmit precise geolocation data to a central government entity.

But, if you start having aggregated analysis from three or four different private entities, how do you make comparisons between those within a city, right? And how do you ensure that it's all accurate, right? So, one interesting solution and we're seeing more and more data trusts. You know, companies that are formed specifically to sort of correlate individually identifiable data from different sources and aggregate it together and then provide analysis to the government entity. That might be a potential solution here.

But without that, I mean, this is what L.A. DoT or others in the same sort of situation would probably say, right? We want to be able to make comparisons between all of these different companies. We want to be able to check our work and not have to rely on the tech companies, who after all have that individually identifiable raw data to begin with.

So it's just a question of which entity you trust. People don't trust my character. I totally agree, yeah. Maybe I'm just not characterizing that correctly. I don't know. No, no, I think you did actually, very well. Okay.

So, a couple other questions, and I know we're revisiting, you guys have gotten, I think you've touched a lot of the big issues,
so I feel like I'm just asking you to go a little deeper on this de-anonymization here. Given what we know about the ability to de-anonymize, right, mobile location data with relative ease,

01:49:32.034 --> 01:49:44.965
what are the legal responsibilities, or maybe ethical responsibilities, I don't know, responsibilities of location data resellers, you know, is that well defined in the law? Does it need to be well defined in the law?

01:49:44.994 --> 01:49:49.944
Do we need to have a list of them that have a green check on Angie's list,

01:49:49.944 --> 01:49:51.414
and the other ones don't? Like,

01:49:52.675 --> 01:49:52.854
you know,

01:49:52.854 --> 01:49:53.154
because,

01:49:53.185 --> 01:49:53.454
I mean,

01:49:53.454 --> 01:49:54.295
I'm a tech guy,

01:49:54.295 --> 01:50:00.145
and I know if you throw enough geo-nerds at something,

01:50:00.385 --> 01:50:00.984
they're going to solve the problem, and if you give them the,

01:50:00.984 --> 01:50:06.055
the task of enriching the data so that, it's de-anonymized,
they just do it,
825
01:50:06.774 --> 01:50:07.164
you know,
826
01:50:07.164 --> 01:50:09.534
and they're just doing what the boss tells them to do.
827
01:50:09.840 --> 01:50:10.260
So,
828
01:50:11.215 --> 01:50:11.425
you know,
829
01:50:11.425 --> 01:50:12.204
we're also,
830
01:50:12.595 --> 01:50:12.954
you know,
831
01:50:12.954 --> 01:50:17.904
work in AGS, EthicalGEO initiative is working with
832
01:50:17.965 --> 01:50:20.875
our friends at the Geovation Center in London,
833
01:50:22.194 --> 01:50:23.784
their Benchmark Initiative
834
01:50:23.814 --> 01:50:26.845
on an international location Charter and this is a big issue,
835
01:50:26.845 --> 01:50:27.175
right?
836
01:50:27.420 --> 01:50:37.194
You know, what are the best practices? What are the principles? What are the
guidelines that we should be asking all companies to live by? And are they just ethical
guidelines or should they be in the law?
837
01:50:40.050 --> 01:50:49.824
So I've asked like 12 questions in there, and that's more of a manifesto and a ramp than
a question but does anybody want to chime in on that? Stacey, go ahead. It's a great
question and
838
01:50:49.854 --> 01:50:55.284
I'm seeing some of the Q and A chat, which I don't know if all the attendees can see that.

Chris

but I can. No, but there's some, yes.

There's some questions being thrown in around whether we anticipate anonymized or aggregated data to be exempted from a forthcoming privacy law, location data is typically not considered to have privacy risks. But it is worth broadening the scope of the question a little bit beyond identifiability because there's also sensitivity, and there are ways that location data can be used that doesn't necessarily identify someone, but can still be unexpected or potentially harmful.
And I think a good example of that is this case out of Massachusetts from a few years ago around geofencing abortion clinics so that the advertising intermediary could send content to people whose phones had been detected to be in those locations.

You know, encouraging them not to get an abortion, or whatever it is, just send content to the phones that have been in a place. That can be done with that re-identifying anyone or knowing the identity of anyone, or even using that data that doesn't, that isn't persistent

overtime, because you can send a geofence alert at a point in time, without even necessarily collecting the location data, right? But it's clearly a harmful use case, right?

It got banned by the attorney general in that state, and I don't know of any company that would do something like that,

right? But I do know that most companies are thinking through similar types of situations around how they should deal with data around schools clinics, right,

and dispensaries and other sorts of political events in ways that don't necessarily identify the person, but have to do with the use of that data for further things.

Do we want to receive politically targeted ads on our phones based on the fact that we went to a rally the week before, right? So these are issues that I think are still being sorted out.

And on the anonymization question,

the question is whether this is going to be addressed by a law, Chris? Sorry I went off on one. If you think one's coming in or who's working on it?
Yeah, there are some methods to legitimately, from what I understand at a technical level,
and I'm not a technologist,
right, there are some methods that can adequately de-identify or anonymize data to within an acceptable level of risk.

or to eliminate..
Differential privacy, statistical methods.
..adding statistical noise,
redacting the dwell locations where a device is located at night, redacting sensitivity,
making the data less precise,
you can toggle the precision to make it less precise to a city level,
rather than a street corner level.
You can take a look at the persistence, right? Maybe you don't need the, every ten seconds for, you know, a developer app to be pinging for location data, maybe it's enough every day or every half hour, or whatever it is, right?
So, there's all these different ways that you, kind of, reduce risk, including through administrative safeguards, right?
We saw problems with ride-share companies in recent years where there was access to a God node in one of them famously right where people could see where all of the devices were going in real-time.

That’s, I can't imagine a situation where that's going to be necessary, right? So you need administrative access controls within a company so that people can't look people up. All of these things go into identifiability and risk management.

All right, Chris? Go ahead, Kevin. I see that you want to chime in. Yeah, a couple of thoughts. In terms of the, you know, data broker, if you will, for lack of a better word.

I mean, I do, I believe it was the Vermont data broker law that referenced location information in the recitals but didn't actually included in the definition in the law itself, which I thought was interesting.

I do think though, that, we will see more of that and the challenge will be as we've talked about, how do you define that, right? I mean, companies have so much location information and they're using it in so many different ways,

how do you define that someone is? In Vermont there is a requirement to register, but there could be other requirements that you impose on that. So I do think there's a real challenge with that.

I'm not a technologist either, and I don't fully understand, I read different reports about how easy or difficult it is to anonymize certain data sets and identify a particular person, and I don’t,

you know, I think that's going to be a really tough question, and I do think it's going to take an enhanced combination of law and policy and technical folks and operational folks to come up with a solution that addresses the risks, because it really varies,

and that's one of the other aspects of location privacy. You know, it covers so many different risks, right?

I mean, it can be used in so many different ways, whether it be someone stalking you, whether it's someone making decisions about your insurance, or in the geofencing case that Stacey mentioned.
I mean, there's so many different aspects to that. As you and I have talked about, you know, around ethics versus the law, I think this community is so large.

I think it involved so many different groups and professions and industries and technologies that, who does the ethical guidelines apply to? And how do you, not enforce them, but how do you even get any, sort of, you know, buy-in to all these different groups?

And I know the open-source community is dealing with that on software and licenses and how to enforce a license that may require someone to use their software for an unethical use or not to use it for things that are unethical.

I mean, the challenge is very significant. So, for me, you know, you need just to start and think with the law and then build ethics around it. Maybe around, particularly segments of the group, the geospatial community or particular applications. But, a broader set of practices, I just find really, really problematic, particularly when you try to do it on an international scale.

So, what are the prospects of a new U.S. federal location privacy law, that may be the wrong question, and who's thinking about it, like, who has a draft sitting on their hard drive.
because that's what they do at night when they're watching Netflix, like, you know, who's thinking about this sort of thing? Stacey, you lit up your mic, you're the first one. You win. Are you the one?

I wish. I would copy and paste half of the GDPR into this. No, people are definitely thinking about it, okay.

So, Senator Cantwell and Senator Wicker on the Senate Congress Committee, Chair and Ranking Minority Member are thinking very hard about this, and have location baked into their comprehensive privacy bills from way back in 2019 before COVID changed everything.

Those are still on the table. I mean, really where a lot of the political will, I guess, fell apart were around non-privacy issues.

It was really about preemption and how the law would be enforced, which impacts the business community in a big way. But it's not really, there was consensus on a lot of the underlying privacy restrictions that ought to exist.

Senator Wyden is certainly thinking about this, so it's been reported that Senator Wyden and his staff are drafting a bill that would restrict law enforcement agencies from purchasing location data as an end-run around getting a warrant.

I would expect, get bipartisan support,
right? That's a very clear thing that there isn't much disagreement amongst, even amongst ad tech companies that are in some cases, providing that data, they agree.

So, yeah, it's definitely being thought about. I don't know that I anticipate a location privacy law.

It could happen, but the sectoral laws that I see more momentum around at the federal level are around biometrics and health data.

I'd be surprised to see location privacy law because it just gets into this, kind of, rabbit hole of a question of how do you define location?

How do you make principal distinctions between location and other types of privacy intrusions into private life when they're not based on latitude-longitude or GPS, right? And how do you enable all of the good things while restricting others?

So, lots of people are thinking about it, but I would expect it to become part of a baseline consumer privacy law in the next 4 years, rather than a stand alone. Great. Kevin, I saw you lean forward.

Yeah, I mean, I agree with what Stacey was saying.

I mean, there's been location-type, location has been included in privacy law drafts for federal privacy legislation for probably 8 or 9 years now, right?
Wyden’s been pushing it and others have as well, Markey I think had something a number of years ago. I mean, it's been, it's been around. I will tell you the one thing I say, and I agree,

I don't think there's going to be a location privacy law at the federal level, and that's probably going to be a problem, because I don't think a lot of aspects of the geospatial community who are collecting and using data are, they're not following it, right?

They see it as a federal privacy law so they don't they don't focus on that. And so, the discussions being taking place around some of the other issues, and location is either not being adequately discussed or defined and it's sort of moving through the system. Now

maybe because of COVID-19 and some of the other things we're talking about, that'll change, but that's been something I've observed. If it doesn't say geospatial information, we're going to stop this privacy law then people aren't part of that discussion.

And that's an issue. Stacey, I did want to ask you though, because I think it's a fair point that it's really hard to have something like location privacy, like you do with facial recognition or biometrics.

But don't you still have those same challenges that you described even if you embed it into a federal privacy law? Don't you still have to define it, you still have to deal with those, not just stand alone? Absolutely.

I mean, the most common way that I see location being incorporated into both proposals and the bills that have been introduced is by sticking it into a section on sensitive data.

So, there's not a 100%,

but fairly good consensus that most privacy laws should include some form of heightened restrictions around sensitive types of data,
which is usually political, sexual orientation, race, ethnicity, religion, and by heightened restrictions, that usually looks like opt-in, affirmative consent. And then some combination of other restrictions, data protection, impact assessments, for example. Most of the time I see location data just sort of stuck into that list as a sensitive category of information. And it makes a certain amount of sense because the Federal Trade Commission, for example, has said that location data is a sensitive category of information. Location can certainly reveal a lot of sensitive information, right? If you have persistent location then you can infer someone's religious affiliation or their political affiliation based on where they're going and their characteristics and their habits. So it makes a certain amount of sense, but I think one of the challenges is that it isn't always amenable to affirmative consent. Right. Nor is affirmative consent always good enough, frankly, from an advocacy point of view, right? Do we want to live in a world where you just have to check 'yes' to everything, right? So if you do it wrong, consent can be this unwieldy, insufficient safeguard to begin with.
But aside from the problems with that, it's not practically possible in a lot of situations with location data.

So, it's possible in the mobile app space, and you could get to a really good legal regime for mobile app and mobile app developers and their partners. But what about location collected from wearables, location selected from IoT devices that don't have screens, location based on the identifiers emitted from connected vehicles. What do you do with license plates and facial recognition and everything else? One solution, you just ban all of that, right? But that's maybe more of a reasonable approach in facial recognition for the reasons Jacob talked about, but for everything else maps, addresses, license plates, everything where there isn't a screen, and you really can't give affirmative consent or maybe it's a family device, right?

Then, an affirmative consent role is just going to make all of those use cases practically impossible.

So, what we see in the E.U. around location data is, it's been kind of bifurcated, so some location data under E.U. law requires affirmative opt-in consent usually when it's done through mobile apps right? And they're sort of developing on that, but they've taken a couple of actions against location marketing companies, the French DPA, the CNIL has taken a lot of action here. But there's another subset of location data, which is data sets based off of the mobile identifiers that are emitted from phones,
so Mac addresses.

This is companies like JCDecaux and Bumbee Labs in Sweden. The Dutch DPA has been very involved in this.

So, when you're talking about airports, stadiums, and retailers who are sweeping via their WiFi networks, usually for the identifiers coming from phones, you can either not do that at all, which is one approach, right?

If you are going to do it to a certain extent because you believe that there's value in physical spaces, being able to know how people are moving, you can't base it on consent, because it's not technically possible, we're going through a screen, right?

You're the identifiers that are being given off and you're collecting them. So, what's the right approach there? And under the E.U. it's been, those companies have used a legitimate interest-lawful basis, rather than a consent-lawful basis.
And what that means is, they do a complex balancing test where they say, okay, there is value to doing this, you do have a business interest in knowing how people are moving around in a space. But there's an intrusion-upon-privacy because these are persistent identifiers.

So, if you're going to do it, and if it's going to be legal, you have to immediately anonymize, delete the data after 24 hours, and you can't track people over time. You can track them within a day and maybe one day, maybe two day, maybe, it's all sort of a little arbitrary, the timeframe, but short-term, okay. Aggregate analysis, okay. But you can't keep the identifiers and you can't track people over time, and that's a judicially created balancing outcome, not based on consent. I think it's a good outcome, and I think we'll see more of that for things like that, like connected vehicles or any other context where you can't get consent. So, very long answer, sorry.

No, it highlights the point that one, people are looking at location as being sensitive in many instances, and there's a heightened scrutiny. And as you said, applying, you know, some of the fair information practice principles, even more, strictly, even though they may not apply to location information for lots of different reasons, or they may not be the best way for location information, right? So, there's that challenge. And then it gets to understanding the technology and the applications at a granular enough level so that you can apply them differently, whether it be through regulation, or legislation, or the courts or whomever.

And that's that's the type of discussion that, you know, we're not having here now, I don't think and Stacey knows better than me, but, you know, we're not having that type of discussion here now. But, you know, things are working through the system, whether it be court cases, whether they be legislation or bans or whatever it is. And that's yeah that's what we're facing.
Yeah, I mean, I totally agree the level of discourse in the U.S. is dramatically higher than where it was a year ago.

But I think it's still not high enough that people who are really technical experts and geospatial scientists, who should feel comfortable that we're not going to end up with a law that unintentionally hinders a lot of really good legitimate use cases, or it doesn't impact the bad use cases, right? Yeah. I just wanted to jump in about the issue.

I think they're like, at the ACLU of Northern California, we've long resisted drawing distinctions and privacy laws including sensitive information, not personal information. There's two reasons for that. One, is that that distinction is, in many cases, a justification for reducing the privacy protection associated with quote unquote, non sensitive, personal information.

And so, it's a sort of a distinction created in order to reduce protections for certain kinds of information. So that's one thing. The question that we would ask is, like, why not protect everything with strong protections.

But at a substantive level, I think it's worth, kind of, being clear minded about what information is collected about all of us is actually non-sensitive.

I mean, the categories of sensitive information that are often specified are health information, financial information, you know, sometimes geolocation information, things like that.

And if you think about all of the information that is gathered as we use mobile devices, you know, our laptops, computers, et cetera.

Sensitive information is often inferable from a lot of that information and, you know, there's some aspects of these kinds of claims, which are pseudoscience.
You know, there's a lot of claims being made that people's emotional states or their mental illnesses, or like, emotional or psychological vulnerabilities can be inferred from the details on how they interact with the website or something.

Whether or not they have COVID-19. Exactly, that too. Some of that is pseudoscience, or at least not justified yet, but I think some of it is real, and just to sort of be specific, you know, Stacey talked a lot about how location information, if you go to a clinic or a place of worship can reveal sensitive, personal information. That's certainly true of our browsing activity, right?

I think probably, all of us have searched for a medical condition, that we were concerned, that we or family member potentially had, or searched for symptoms that we have looking for some kind of hint that is the diagnosis. Search history, browsing activity, certainly private communications, like messages, emails, or even the metadata associated with those communications, I think could reflect sensitive personal information as defined.

And then, one example that I found sort of terrifying is there's a, Uber actually has a patent application based on detecting whether somebody's intoxicated based on their use of a mobile app.
And I think it's not crazy to think that somebody who is intoxicated is going to use a mobile application differently and that difference is going to be detectable by the application itself.

But if you do that, and that is possible, then the sort of like, how someone scrolls or how someone taps on their mobile phone could actually be an indicator of alcoholism or other kinds of health conditions.

And so, I think the distinction between sensitive and non-sensitive, personal information is, kind of like, blurry and porous at best.

And so, I haven't seen a distinction between those two categories that takes that porousness seriously. And for that reason, I think it's better to have a single category of strong protection for personal information. Yeah,

I mean, I appreciate what you're saying. We've had so many references to help. We haven't really discussed how specifically, one of our EthicalGEO fellows, Father Michael Rozier, from St. Louis University, I guess he's also a professor.

Michael Rozier, you know, he always gave the example of HIPAA, where all of your health data is protected by HIPAA.

But the mobile location data that shows that you walked into an AIDS clinic at 10a.m. on Tuesday, isn't protected by HIPAA at all and could be picked up by any ad tech company and re-sold to whoever. So that's kind of an interesting issue. We do have a question that came in from the audience about specifically,
you know, health data. I think their concern is, you know, what are the effects of government reliance on private contractors and companies to manage geolocation and health data, but you can twist that question two or three other ways, you know, when there's a big marketplace of that location data, from it, could be inferred your health status, or your concerns about your health status or whatever, you know, what are the public or private access issues around that? And you just covered that Jacob? Does anybody else want to chime in on health, maybe the health dimension of this or is it just good enough that we noted it for the audience because it is not protected by HIPAA? I mean, Jacob's example around the patent for whether you're intoxicated kind of gets you into also thinking about behavioral biometrics, which is kind of a fascinating thing. I think it turns out that the way that we use our phone, and the way that we're standing and the way that you type can also be used as an identifier, at least in the short term, a method of biometric identification, which is really, really interesting. I'm going to do a couple more questions as we bring this to the end. I think you guys have helped us uncover so many issues. There's a great question that came in from the Facebook live audience. When lawyers and policy makers are writing policies and regulations to ensure citizens and consumer privacy is big tech at the table, or I guess I'd say,
I'm sure they are but, in what ways is big tech at the table to help explain the technology to the policy makers and the lawyers? And what incentives do big tech have in providing that information if it's really going to just make it harder for them to use the data, or sell that location data? Do you have an invested interest in not educating policy makers and lawyers or do you see them being pretty forthcoming, and, you know, some might say on the offensive, but being proactive in helping educate people? And I do want to broaden that beyond Apple and Google, you know, people that sell phones, you know, there's people who sell drones and their satellite companies, and, you know, which parts of the landscape, tech landscape are being proactive and helpful and which ones aren't.

Good one. So, first of all, no, I don't think that there's a vested interest in not educating policy makers. Definitely not. It's in everyone's best interests that policy makers and lawmakers, particularly, are well informed and know what they're doing.

I think one of the challenges that I've seen is companies, especially larger companies just tend to have a divide between their technical experts and their product engineers and their lobbyists or public policy experts, or the people that are willing or able or designated to go in and talk to policy makers.
Sometimes that’s just bureaucratic.

Sometimes it’s self-interest. I know a lot of companies, for instance, are very hesitant to go talk to the FTC for example, even though they could probably do a lot of good, because they’re sitting in a room with a regulator, and if they say the wrong thing, or if they feel like they say the wrong thing, they’re going to bring scrutiny and attention down on them. So, you know, same with going into and talking to policy makers.

And so you often get things that are just talking points and then you also get things that sound like talking points, even though there’s real legitimate technical expertise behind it to justify that point, but ends up sounding like a talking point to a policy maker, because the person that they’re talking to doesn’t have the technical background, right? So, my advice to companies is usually to make sure there’s as much cross-pollination and discussion internally within the company as possible. So that the policy experts are as well informed as they absolutely can be, so they can inform lawmakers. Yeah. Yeah, just to jump in. I agree with that and I think that there is a lot of helpful information that comes from technology companies with respect to how the laws will affect the technology and then, sort of, what’s happening on the ground. I think it’s really important that product expertise, the market expertise, and the technical expertise be brought to bear on the policy making process. I will add that in my experience, there’s often this notion that there’s a privilege of people with deep technical expertise in these conversations that I think is a little, has not been born out of my experience. At the ACLU, we have technologists who work on the speech, privacy and technology team at ACLU National. EFF has technologists, their own staff, that build tools and also advise on policy questions, and there can be fairly widespread agreement with respect to the deeper technical details, and then vast disagreement about what the right policy answer is, and I think that is often a result of the fact that while technical expertise is important, it actually, it is sort of underdeterminative in the sense that having technical understanding does not answer the policy question for you. What you need to answer the policy question is policy judgment and to decide which communities to protect, whose interests are favored and there you get into a much more murky area where the incentives of the particular legislator or policy maker etc. come into play, and you know, the priorities of the regulator if you’re talking about FTC. And so, yeah, technical expertise doesn’t answer policy questions as a general manner but it is a very important input to those policy questions. I agree with that and I’ll say, a potentially bigger
problem is less having the technical expertise and more having the knowledge of business models and the data flows involved in the modern ecosystem, internet transactions for example, how they work, how social media platforms work and what those data flows really look like because most lawmakers are considering not just the privacy implications of the laws they might right, but the economic implications. In my mind, it’s very challenging to write any kind of privacy law that isn’t going to impact some private sector industries, some public sector industries, some business models and not other business models. So if you’re concerned about anti-trust or if you’re just concerned that you’re going to just accidentally wipe out the ad-supported internet, and force us all to pay-walls or cookie banners, those are legitimate concerns. You have to understand the business models in order to make policy judgements about which ones you’re okay impacting or eliminating and what that process is going to look like and whether it’s going to be supplemented by more privacy innovation and new and different types of business models that are going to be more privacy protected. And this is just coming from my advertising background, right. This is at the crux of most privacy law proposals we see. Kevin, go ahead. And yeah, so to follow up on that because I think Stacey made a couple of excellent points. I think with location in general, the issue is that most of it is still wrapped up in the advertising discussion and many of the big companies at the table are looking at it from an advertising standpoint and their trade-offs, their understanding, their business models are different than many others that are using location technology. But because for a lot of those businesses, one, they’re smaller or they consider themselves in different sectors, they aren’t necessarily part of the same trade associations, or going to the same meetings, or going, even, before the same committees, right, because that’s an important part. Their voice isn’t being heard or they’re not contributing to the discussion. And so, a lot of the folks, Chris, that you and I know that are big players, if you will, in the geospatial community, they’re looking at other matters that are more important to them and they’re not focussing on privacy, and so, they’re not part of the discussion, they’re not, as a question said, at the table helping them explain the technology, and as Stacey said, this is what’s going to happen, if you do X, this is what’s going to do us, and maybe you want to do that, maybe from a policy standpoint that’s fine, but the unintended consequences are X, Y, and Z. And that discussion, I'm not sure, is taking place as well as it could, around location privacy in general.

Yeah, I agree. And companies have to be more forthright about it too. I mean, from most company representatives or trade association representatives, that we speak to are not willing to say, you know, here’s the slice of business practices that are more risky and more privacy invasive and here are the ones that are less, and here’s how we can make some principle distinctions about what how a privacy law might impact because it's not in their self interest, they’d rather just say no. Right.
But that's not going to create practical ways forward. Right
So,
as we wind down toward the top of the hour,
you know,
it's a confusing landscape and I've got three,
you know,

If I'm a lawyer and I'm interested in this stuff, where should I get involved? I mean, other
than FPF, The Center for Spatial Law and Policy, and the ACLU, right?
I mean, obviously, they should be members of all three. But if I'm a lawyer, an active
lawyer out there, or maybe a law student coming up through the ranks, and I think this
is the future. Where should I be involved?

What should I be tuned into? Who should I be following, other than you three? What
kind of guidance can you give folks in the legal community?

Yeah, join up. Yeah, for sure we have law firm members that are part of our community
and our advisory board. If you're starting out, I think, in your career, you're a new lawyer,
I think that the IAPP can be a great resource and membership community. What's the
IAPP?
The International Association of Privacy Professionals. This is mostly in-house, general
councils and practicing privacy professionals at companies, and law firm members, and
a lot of
it's been professionalized,
1060
02:25:29.665 --> 02:25:42.834
right? So, there's a certification test and all of these things that's, I think, a very different
world than the advocacy world, where you're looking at organizations, like EPIC and
ACLU which are, which also have a lot of activity that they're doing.
1061
02:25:43.284 --> 02:25:45.415
Any number of these things are great ways to get involved.
1062
02:25:47.844 --> 02:25:57.805
Oh, yeah, go ahead. Kevin. I agree, IAPP is a good resource. I think the legal community
is,
1063
02:25:59.245 --> 02:26:00.204
I'd say,
1064
02:26:00.204 --> 02:26:08.784
woefully unaware of the legal and policy issues around data in general, and I include
privacy as certainly part of that data protection,
1065
02:26:08.784 --> 02:26:09.895
but intellectual property
1066
02:26:09.895 --> 02:26:10.254
rights,
1067
02:26:10.254 --> 02:26:10.524
data,
1068
02:26:10.524 --> 02:26:12.264
quality and liability issues,
1069
02:26:12.684 --> 02:26:14.274
the national security issues.
1070
02:26:14.575 --> 02:26:28.944
I think there's a whole set of laws, and you and I have talked about them before. I mean,
I think that's where, you know, more lawyers need to be paying attention to and that's
involved some product liability, some intellectual property,
1071
02:26:28.944 --> 02:26:29.995
certainly privacy,
1072
02:26:29.995 --> 02:26:31.764
but those set of issues,
and to Stacey's point
and Jacob's point, understanding how data goes into an organization, how it's used,
what the ecosystem,
how it comes out,
whether it be location,
whether it be medical or health is going to be increasingly important
both for the public and private sector. So, and, you know, there are different, there's no sort of course of study,
I don't think you can go to do that now,
But within the ABA or IAPP or International Bar Association, or others,
there are folks,
you can take, you can go to classes and take things on the legal side in addition to sort of,
outside of that,
you know,

02:26:31.764 --> 02:26:33.354
and to Stacey's point
1074
and Jacob's point, understanding how data goes into an organization, how it's used,
what the ecosystem,
how it comes out,
whether it be location,
or whether it be medical or health is going to be increasingly important
both for the public and private sector. So, and, you know, there are different, there's no sort of course of study,
I don't think you can go to do that now,
But within the ABA or IAPP or International Bar Association, or others,
there are folks,
you can take, you can go to classes and take things on the legal side in addition to sort of,
outside of that,
you know,
with industry groups

02:27:08.604 --> 02:27:13.704
and things to really learn how those industries are collecting, using, sharing, and
storing data.

Yeah, those are all really great suggestions and I completely agree with them. I would
add, you know, thinking about pursuing opportunities inside of regulators. I spent
almost five years as an attorney at the FTC.

02:27:31.735 --> 02:27:44.604
I actually did a little bit of privacy, but not very much. I focused largely on consumer
protection, false advertising cases, and interest mergers, but just being in FTC and
seeing how the agency operates,

02:27:44.604 --> 02:27:55.614
even if you're not doing work inside the division, the division of privacy and identity
protection, that is the sort of core privacy regulator within the FTC, you're going to see
those cases, you can see how the agency works.

02:27:55.795 --> 02:28:04.465
And I think it's really helpful to understand how the privacy regulation works inside that
agency. State agencies I think are also a really great place.

02:28:04.495 --> 02:28:17.485
Obviously, the California AG is currently enforcing the CCPA, but there are other state
AGs that do privacy law enforcement, either through their unfair deceptive practice
statutes or potentially through new state level privacy laws.

02:28:17.514 --> 02:28:27.805
Even if those state level privacy laws are more sectoral than, like, the CCPA might be.
Kevin mentioned the Vermont Data Broker Law, or the Maine ISP Privacy Law.

02:28:28.645 --> 02:28:40.975
There are a lot of state level privacy laws that are enforced by state AGs, which are a
little bit narrower than a broad based consumer privacy law, but I think are also really
great places to get experience with privacy law.

02:28:41.905 --> 02:28:56.725
And then, finally, in-house is, I think, a really great place for people who were early in
their careers, and later in their careers as well to gain deep market knowledge and
product knowledge,
and then also legal expertise around what rules are in place. And I think that's one where the sort of the market for lawyers is very good.

1098
02:29:08.459 --> 02:29:17.545
There are a lot of in-house opportunities for privacy lawyers and trust and safety lawyers. And so I think that's a place to keep in mind as well for people who are earlier in their careers. Thank you very much. You know, we started with COVID-19, and contact tracing, and we've covered far afield from that. I mean clearly the implications for what happened before COVID-19 is shaping how we respond to COVID-19, and what we put in place during COVID-19 will shape our response to whatever the next exigency is. I really want to thank you for giving us your time today. I know your time is probably your most precious resource so thanks for sharing it with us and the community. AGS isn't normally where lawyers come and hang out but maybe we need to start a Law and Geo drinking club, well I guess it would all be virtual happy hours right now, but I certainly feel after time with you, I could play a lawyer on TV, at least as a bit-part on Law and Order for a few minutes. So thank you for your time and expertise. I'd like to thank you, I'd like to thank our audience for taking a couple of hours out of their time to join with Ms. Stacey Gray, Mr. Kevin Pomfret, and Jacob Snow, and I would be remiss if I didn't thank our sponsor, Henry Luce Foundation. Without their support, none of this would be possible and their support has enabled very important dialogue in educating all of us.

1099
02:30:47.760 --> 02:31:00.805
Before I leave you to your weekend, I just want to point out, not only have we had many sessions in the past that if you go to ethicalgeo.org and click on Location Tech Task Force, you can view all of those recorded sessions.

1100
02:31:01.045 --> 02:31:12.174
But we have another session coming up on September 8th; Tracking Movement through Space during COVID-19 and Beyond.

1101
02:31:12.415 --> 02:31:22.645
So, we'd love to have you tune in and stay with us on all of our future events. So, thank you very much for joining us and have a wonderful weekend. Take care.

1102
02:31:24.059 --> 02:31:25.344
Thanks Chris. Thanks.