Charting the Future: What to Expect from Big Data

Mary Ellen Callahan, Elisebeth Cook, John Grant, Adam Isles, Greg Nojeim, Robert O'Harrow, Marc Rotenberg, Stephen I. Vladeck*

Stephen I. Vladeck (SIV): Marc, I'm going to turn it over to you to introduce the audience to the first case study.

Marc Rotenberg (MR): Thank you. With our first case study,[1] we're trying to pull in the various elements of detection technologies and we're also beginning with the premise that what makes these detection technologies so fascinating is that they generate a lot of digital information. That digital information can be analyzed and scanned, and we can apply rules and make certain determinations based on what we are able to learn about people. We've upgraded our CCTV system so that it now has facial recognition. We've introduced a new technology called "terahertz scanning" which can detect material composition at a distance. For example, if you are worried about people walking around the street with explosives, this is a device that will allow you to make that determination. And for this case study, I got to coin an acronym – and it is the Second Generation Municipal Security Network (SGMSN). I'm really proud of that. It took the better part of a day. So I'll turn it back to you and just say that the key to understanding this problem is that we're no longer in the analog world; we're in a digital world. There is a lot of information generated and we need to make some decisions about how we are going to use it.

SIV: That's a great introduction Marc, thank you. Let me start by throwing a fairly open-ended question to the panel: Given the scenario that Marc has laid out, what do you see as the principal privacy concerns with the system? If you are approaching this problem from the government's perspective, what is your concern? From civil liberties groups, what are your concerns? From the perspective of the manufacturer of this technology, what's your concern? Where would you start in even trying to figure out how to create privacy protections for Mark's new SGMSN?

Greg Nojeim (GN): There are no wallflowers up here on this panel so let me just jump into it. When I read the scenario the first thing that jumped to my mind was the end of anonymity – that you wouldn't be able to walk down the street anymore anonymously because there would be this back-end data that

---

* What follows is an edited transcript of a panel titled "Charting the Future: What to Expect from Big Data," held as part of the *Journal of National Security Law and Policy*'s February 27, 2013 symposium on "Swimming in the Ocean of Big Data: National Security in an Age of Unlimited Information." For an introduction to – and overview of – the panel, see Stephen I. Vladeck, *Big Data Before and After Snowden*, 7 J. Nat'l. Security L. & Pol'y 333 (2014).

1. The first case study is reproduced as Appendix I to this Transcript.

could be used to figure out who you were and then there is going to be some learning about what you were up to based upon what you were concealing under your clothes, which could be revealed by its chemical composition at a distance. You wouldn't know that this was happening.

The second thing that jumped to my mind immediately was whether there is a Fourth Amendment "search" going on. And I thought about two cases in particular. One was the *Kyllo* case where the Supreme Court said that the government's use of a device to detect heat emanating from a house and to use that technology to make inferences about what was going on inside like growing pot was a search.[2] And then the *United States v. Jones* case came down about a year ago, where the issue was about whether the police need a warrant to attach a GPS device to a vehicle and to track the vehicle, and the case went down on trespass grounds.[3] The Court said it's a trespass when you attach the device to a vehicle but the interesting opinions in that case were the concurrences, where they said it didn't matter that there was a trespass. What mattered was the persistence of surveillance and the invasiveness of it, and that those things together could turn that surveillance into a search.[4] So I looked at the case study and I said, well gosh, this looks pretty persistent, and it looks pretty revealing and invasive, maybe it triggers this search criteria under these concurrences in the *Jones* case.

SIV: So I want to bring Mary Ellen in, but let me throw in a wrinkle first. A staple of the Supreme Court's Fourth Amendment jurisprudence is that the police are allowed to see without a warrant things that private citizens could see themselves using existing publicly available means. So it seems that, as this technology proliferates and as it is increasingly deployed by private actors, there may be a counterargument on the Fourth Amendment question that such surveillance is in fact a variation on the plain view doctrine, not because it is in "plain view" as a matter of common sense, but because it is plainly viewable to private citizens.

Mary Ellen Callahan (MEC): I think that is a factor. I mean the U.S. concept of privacy is exactly that, if it's in the plain view if you are outside the home then it is in public and it's possibly discoverable, so to speak. I think Greg is exactly right that there are two different issues here. One is Marc's brilliance of designing this hypothetical technology to also detect *chemical* compounds. I think that's a different issue, but let's just talk about if CCTV was able to have this facial recognition associated with it. I think that the factors that should be considered there are ones associated with persistence and with ubiquity. And from a privacy perspective, I'd worry that we're collecting this information, we're storing it, and any time you're having this broad collection of information with a possibility of going back and looking for information associated with a

2. Kyllo v. United States, 533 U.S. 27 (2001).
3. United States v. Jones, 132 S. Ct. 945 (2012).
4. *See, e.g.*, *id*. at 957-64 (Alito, J., concurring in the judgment).

threat, with violence, with a crime my concerns would always be the *secondary* use – what are you going to use it for, so you are collecting this information and what is it being used for. Are you sharing it with other people? And furthermore how long are you keeping this information? I think that those factors have to be part of the analysis here because, yes, we have the capability of collecting every activity that takes place in the world given existing technology. But I think we need to think about the uses and the sharing and what our restrictions are. Even if it is a private sector individual having this data, having the scoping defined is still important.

SIV: Beth, do you want to jump in?

Elisebeth Cook (EC): I do. I was going to accuse Mary Ellen of looking over my shoulder and taking exactly what I was about to say here. What struck me as I read this is that there is an absence of particularized suspicion for any sort of the collection. It's likely that you have a high percentage of U.S. person information being collected, so putting aside the Fourth Amendment questions that are raised on whether it's a search or how we address the *collection*, it also matters what the *retention* of this data looks like, what analytics are being done with respect to this information, what subsequent dissemination is happening within the government, those were the issues I really jumped to.

SIV: Bob, do you want to jump in?

Robert O'Harrow (RO): I would like to play a slightly different, very, very non-lawyer role here in trying to look at this a little differently than the very well-articulated legal concerns. First of all, I think in theory in a platonic sense having cameras that can detect things, precisely identify people, and identify potential chemical bombs and threats in theory and on paper is a great thing. And we want to maximize the use of technology and data mining in that way and in other ways to maximize our freedoms and securities and so on, that's on paper. The flip side of it is it's clearly a tool to impose – not on privacy which I have used less and less over the years because I think it's a tofu word that takes on whatever flavor you want to give it. But I like to look at it more in terms of autonomy and the allocation of power. This creates a new way to exercise power against an individual that they may not agree to, they may not have ever agreed to and the person exercising the power may really have no right to do it. So I view it that way and finally I think that we should consider that if it is going to be used and if we agree as a society to allow this kind of technology to be used then we have to figure out a way to have very serious criminal penalties for misuse, rather than incredibly namby pamby, vague, and almost never truly applied penalties that we have now so that we could maximize the use of technology and punish people who misuse it.

SIV: So, John, let me bring you in here because I want to ask a specific question pivoting off these last couple of comments. Is it possible that part of how we answer this question from both the legal and policy standpoint is going to depend upon whether there is a human operator who is actually sorting through the images with the facial recognition software, versus a machine

algorithm that is running by itself? If so, is it actually perhaps counterintuitively possible that it's more privacy-protecting to use facial recognition technology and have it pull out just snippets of 12 hours of video data as opposed to having an individual person literally *watching* all 12 hours of that data?

John Grant (JG): The question of machine analysis versus human analysis or human checking really boils back down to "does it work?" That should be the first question that we ask when we're considering this stuff. Palantir does not do facial recognition software.[5] But we've considered other technologies that people want to propose to analyze data to use algorithm analysis of data, and one of the more popular ones recently is social media analysis – and particularly sentiment analysis, trying to derive sentiment from a bulk amount of tweets. We evaluated a couple of these technologies, and I won't name names but we evaluated three of them against the same group of tweets and all three of them came up with completely different analyses that would have pointed in completely different policy directions with what you do.

So I would say, shooting ourselves a little bit in the foot here as a manufacturer of this kind of stuff, don't listen to the manufacturers. You need to be evaluating them yourselves, and that requires a person to be looking at this and comparing it to certain benchmarks and possibly that you have to lead that person in there in order to truly make effective use of the technology and whatever operating procedure you have. And we see this all the time: sentiment analysis is in every RFP for social media analysis right now. And as I said, it's not clear that it works. And so the danger becomes that you end up with what DHS went through with airport security – the machines that they spent millions of dollars installing in airports that didn't work that they ended up taking out because they didn't work and now they are changing out the "naked body scanners," as Jeff Rosen calls them, because they have more privacy protective technologies. So I would say that getting to that threshold question is the key – what Bob said about the accuracy of what you are doing. Does it actually work? Is it finding what you are looking for?

And to the second half of your question, if it does work then we should also consider as we're doing cost benefit analysis for this the privacy enhancing aspects of it. So if you have 12 hours of video tape and you know you use facial recognition on that as the computer looks at it, and you know that John Grant is on five minutes of videotape, then by directing law enforcement or the intelligence analyst to just that five minutes, are you better protecting the privacy of the people who are on the other 11 hours and 55 minutes that nobody actually looks at? What it comes down to is whether there is a significant difference between a person identifying someone in a set of data so in this case a police officer looking at video and saying okay there is a person in this five minutes of video I'm going to tag this person I'm going to mark this person. Is there a

5. Palantir is a software platform for data analysis, used by many government organizations. *About*, PALANTIR, http://www.palantir.com/about/.

difference between that and a computer just automatically tagging everybody in the system? Because obviously if the law enforcement person is making a judgment then they are saying this person is going to be of interest, these other people are not so there is more than just identification going on here, there is some sort of judgment call. But with a computer all it's doing is structuring data, it's just saying this is a John Grant, this is Greg, this is whoever, this is a chair, this is a window, and there is no significance to it. So is there in terms of evaluating the social cost of surveillance a difference between who is making that call?

SIV: Adam and then Greg, do you want to weigh in on this?

Adam Isles (AI): I agree with what John said about needing to look at the usefulness of this: First, is it actually effective? And I think both in terms of effectiveness and appropriateness this ends up being context dependent. So in terms of its use and inventiveness, are we talking about a surveillance or an inspection purpose? Are we talking about looking at a very specific place or people that are walking in and out of that place, or are we talking about walking through a checkpoint at some point and under specific circumstances, because I think you'll find that the accuracy regardless of where technology is headed is going to vary based upon that.

SIV: Is there a difference between whether it's a preventative search (that is, it's trying to prevent something from happening in the future) versus spying on someone who matches a profile of something that happened in the past? Is that a relevant consideration here?

AI: I guess it depends on how broadly you want to think about preventative, right? Are you talking about a subject-based or a pattern-based exercise?

SIV: That's where we're going. Greg?

GN: Just to jump in real quick: John, we're here to talk about not that five-minute segment really that just had John or Greg in the camera's eye. We're talking about the other 11 hours and 55 minutes, that's really what this conference is about. We're not looking for the particular person, we're trying to derive intelligence from this data that was collected maybe while we were looking for that particular person, but now we've decided to repurpose it to use it for something else – and that is why I'm concerned about the collection at the front end.

SIV: I want to get Mary Ellen in, and then I'll get back down to Bob. Mary Ellen.

MEC: So both Bob and John asked questions that I think are worthwhile. Bob said there is rampant misuse of information and then John said the first question to ask is does it work. Based off of Bob's questions, the first question to ask is why are you collecting it – is it for a preventative purpose? Is it for something specific? There is a term that I hate, but it actually may be relevant here – privacy by design. So you go out there and you actually go and try to figure out what you are trying to do because then you can figure out what is the misuse. If you just put up a CCTV and you go and collect all this information

then what happens is people go and say "I could use this for a preventative purpose," or "I've heard there was a crime here, I would love to collect it for that purpose." Or "it would be great to see how many males versus females walk down the street." Once the data is collected, there are lots of people who want to use it, but you've got to define what the permissible scope is first before you go and stage this. And then you also can talk about what's law enforcement access – what are the standards that we are using? Thinking about it ahead of time is important.

SIV: Can I push back really quickly? What you're saying is that "you" have got to define the permissible uses of the data. Can I ask who "you" is in that context? Is it up to Congress to define this context? Is it up to the purveyors of the data? The recipients of the data? Who do you think the responsibility lies with for setting the relevant criteria?

MEC: Well I think it's the people putting up the CCTV. They are the ones who are storing the data; they are the ones who are going to have to respond to law enforcement requests or maybe they are the federal or state government themselves, so I think before you put it up just because it would be fun you as the purveyor need to think about what you are trying to do and what you are *not* trying to do. Again, in this non-particularized collection of this vast information, the concept of secondary use is the biggest hurdle in this process.

SIV: I want to get Bob back in.

RO: To follow on the secondary use idea, it's a dream for efficiency-minded law enforcement and/or domestic intelligence officials for private companies to adopt Mark's unpronounceable system because it creates pool data that they then go request. They are not allowed to collect this data under the Privacy Act and amendments since then, but as we've seen, they're perfectly capable of going and contracting for it.[6] We know this because this is the data that we leave behind in warranty cards, shopper cards, all this stuff that we fill out that is now at Axiom, Lexis-Nexis, etc. This is the fodder for a lot of security systems and so I wanted to point that out. The other thing that I would like to note is that the systems that John mentioned in terms of limiting what law enforcement can look at and saying we're only looking at five minutes not the 55 minutes per hour is a fig leaf that we have to be alert for, because it would actually encourage the creation of these pools of data that then they would tap later.

SIV: Fair enough. Marc?

MR: Sometimes, when you ask a hard question on an exam, people end up writing the answer to the question they thought you were going to ask and avoid the question you are asking. I will say about this scenario that there is a lot going on here that I anticipate will happen – and it will happen in the near future. And it is set up in such a way to drive a discussion to a point where we need to get to in order to engage the next level of debate about big data. Now

6. 5 U.S.C. § 552a (2006).

before I made a personal commitment to address the lawyer shortage in Washington, D.C., I was very much interested in computer systems and rule-based expert systems, and fascinated by the problem of how we process a lot of information. And if I design a system for you and I tell you that a person who walks down a city street late at night peering into the driver's side window of each car he walks by is more likely than not casing cars to determine which one is unlocked that he can get into, and I can now through an enhanced CCTV system sweep the whole city to identify the four or five people at any time engaged in that activity and then notify a local officer, go to this location because with a very high probability we believe a crime is about to be committed. I think that is the world we're moving toward.

I'm not talking about "certainty" (although apparently that's now the standard for Article III standing requirements).[7] I'm talking about something that begins to approach that and I suspect a lot of people in this room understand what the reference is to. We're trying to look at information in a probabilistic way and make some assessments about where we think crime or terrorist threat is likely to arise. And that is where we need to ask some hard questions. Are there limitations on data collection? If I point my terahertz detector at a crowd in Union Station and I'm able to tell that one person is actually walking around with C4, you better believe I'm going to try to get someone on top of that person as quickly as I can. So in a world where this becomes possible, what types of legal constraints and policy constraints do we need to establish?

SIV: That's a great segue because it seems to me that part of the trick here is that most if not all but agree that when you have a terahertz detector that trips for C4, there is no serious argument that a private person walking about with C4 is doing so for some lawful permissible purpose as opposed to someone who might just be peeking into cars. And so assuming someone can come up with a better justification than I just did for that latter activity, is there a way to set up the screening ex ante so that there actually are safeguards in place before you are even *acquiring* the data, where you are only screening for a particular kind of activity where there is some kind of sign-off that that is the kind of activity that we want to screen for? Is that realistically feasible or is it only going to work in the hyper-extreme cases of chemical weapons?

MR: Speaking of *Clapper*, it was very interesting because when the federal Wiretap Act was first established in 1968 and it was seen as extraordinary authority, it was described as an investigative method of last resort – literally. There are a half a dozen predicate crimes that were the only bases upon which you could do electronic surveillance in 1968. Now that list today has grown to several hundred crimes for which wiretaps can be authorized.[8] But I think it's very interesting this moment in time we're at. I think we're about to see another

7. *See* Clapper v. Amnesty Int'l, 132 S. Ct. 2431 (2013).

8. *Compare* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 *with* 18 U.S.C. § 2516 (2012).

wave, and so we need to begin to ask these kinds of questions – for which types of activities would we allow this type of surveillance?

SIV: In that regard, the *Clapper* decision may be the far less important development at the Supreme Court this week as compared to the oral argument in *Maryland* v. *King*, about when law enforcement can take DNA samples from individuals who were arrested for serious crimes.[9] But I wanted to go back to Mark's point. Do the rest of the panelists have views on setting up ex ante criteria where there are certain kinds of technologies at issue? I mean someone peering into windows for example on Massachusetts Avenue at 2:00 in the afternoon seems like a different threat matrix. Is this feasible? Can this be implemented in any practical way? Or can we only really assess these considerations after the fact? Adam, do you want to take the first shot?

AI: To some extent there is sensing technology already out there that does this, I mean it's not necessarily personally identifying but think about the Metropolitan Police Department putting gunshot detection equipment out around the city. This comes back to the point about being context-based. If it's intelligence-based, you are limiting the technology to a certain neighborhood where you know you've got a real crime problem. That's a different proposition than if you are basically deploying a capability city-wide or nation-wide, or if there is some specific event that is going to begin and end that it is being deployed for. Is there also an extent to which you can consent or the surveillance is truly voluntary because you are getting some trusted status as a result of walking through a place? I think that matters. There are two larger points that I think have been briefly touched on that I would want to make. One is the difference between what the government does for Fourth Amendment purposes versus what the private sector does. And the second is a point about the nuance in the technology. There is a capture portion of this that involves a sensor that has a better focal plane array that actually allows you to capture the stuff. But the back-end matching aspect of this is what Marc is really worried about, and once that technology is out there, is there a bigger worry in what the private sector does as opposed to the government, where theoretically at least you have at a minimum policy and potentially the Fourth Amendment to control what it is that is actually done?

SIV: Bob, do you want to jump back in?

RO: Yes, there are rules that should be applied, and I think that we should recognize how the government behaves and the government behaves effectively like a lot of parts of our society which is they'll do as much as they absolutely can if they are not going to be punished for it. So I think we should set up rules and we should spend the money inside the government to hire people that will follow up on this and truly punish people who break the rules that we decide as a society.

---

9. Maryland v. King, 133 S. Ct. 1958 (2013).

SIV: That presupposes that we have some consensus understanding on where the line is, right? Beth, can I bring you back in here? Do you have views about the line-drawing problem in this context?

EC: We've gone from electronic surveillance with full content on the one hand to having technology deployed in Union Station which is akin to dog sniffing, so you have dogs that are trained to a set of behaviors that you are looking at that may or may not alert to individuals who are carrying explosives, putting aside the collection aspect of it. Then we have this misuse notion which I don't think we've come to consensus about what the use is or what the misuse would be, and then I'm envisioning hiring folks to go behind the officers to figure out if they are misusing it – and in order to do that we have to retain the data for longer, we have to create more extensive audit trails. You end up with vast reservoirs of information that appear to serve no purpose except to facilitate investigations of the investigators. So I would like to know a little bit more about how Bob thinks that the misuse is best found in a way that doesn't actually then violate the privacy of individuals a second or third time.

RO: I don't know what you mean by violating the privacy of individuals, but if the government says you can use this to detect people who have C4 strapped on them and you may not use it for anything else, if it's used for any other purpose then that person loses their job, goes to jail, etc.

SIV: What do you mean by "use," though? If it's an automatic scanning system, presumably your point is it should only alert when it detects C4, no?

EC: I just think we haven't really gotten to misuse, which is a few steps beyond what as a policy matter is a good use of the data. Setting up a construct to determine whether *misuse* has occurred is not as simple as it might seem.

SIV: With that in mind, is there any way that I could try to ask the panelists to give their view on what would be permissible use at least of the technology that Marc outlines in his scenario of the SGMSN?

MR: Here is one line-drawing example: airport body scanners were put in the airports to detect threats to air travel safety, perfectly reasonable but of course as a practical matter they also made it possible to detect other materials – notably narcotics – that people could not lawfully possess. Now it's an interesting question to ask whether or not the searches that resulted from the deployment of airport body scanners which resulted in the production of a lot of narcotics evidence were properly obtained. I think there are all sorts of good public policy reasons why you could say "why not."

SIV: Right – if you've got a search warrant for a gun and you happen to find a bomb, you don't ignore the bomb.

MR: The Court of course struggles with these issues; is this plain view? Is this consistent with the original purpose of the search? But to me, that's almost exactly the problem that arises with terahertz, because we might say well yes we're concerned about public safety, if someone is walking around with explosives. Concealed weapons get more interesting of course because there are some scenarios under which that is permissible and other scenarios under which it's

not. So does that provide the predicate for the stop to determine whether or not someone actually has the license to carry the concealed weapon? Terahertz is going to create these kinds of dilemmas.

SIV: Greg, Marc seems to be suggesting that it's going to be very difficult to simply say yes, this is a permissible use, but you cannot use anything else you find by accident. Do you have a reaction to that?

GN: I think it understates the problem. The actual big problem is new authorized permissible uses. That's the big issue. I see no way in this political environment to stop the new uses. So say there's a rule and say it's statutory and the rule is that terahertz technology can only be used to detect weapons, bombs, thing that could destroy. It will never stop there. We're being unrealistic if we think it would stop there because other people will say but drugs are a big problem and so we need to detect them. We can, so let's do it. Some people will say something else is a big problem we need to detect it, let's do it. There will not be a political will to stop the new authorized uses.

AI: I disagree with that a little bit because I think today TSA doesn't have authority collect for narcotics purposes. I mean if it's in plain view and someone has noticed the fact that they are going to walk through just happens to walk through they can't be blind to the fact that it's there but there is nothing in TSA authorizing legislation or regulations that gives them the affirmative authority to look for drugs.

SIV: This is the question I was asking John before: If it is technologically possible to have this technology only alert for the agreed upon permissible uses, would that solve these problems or at least mitigate them?

JG: I think you certainly envision a system where at some point suppose you had CCTV systems, you had a policy or process in place where I am looking for someone and I have proof that they have been involved in some criminal act or something like that, and you say this system does not record until it sees the person that I'm looking for and recognizes it. Now what Greg will say and I agree with this, is that you're still surveilling everybody. So we have to evaluate the actual societal harm of ubiquitous surveillance. I think everybody in this room probably thinks yeah this is terrible we can't have ubiquitous surveillance you know there is a chilling effect, there is a negative social consequence, but everybody in this room also has friends who use Facebook, and probably all of you have lectured your friends on the information they are putting on Facebook or told them to throw away their stupid Borders cards because they are creating a list of all the books that they like and that's our consciousness. But is there proof out there of these negative societal effects of this ubiquitous surveillance? I think we ought to look for that and then go on to say here is the specific harm as a result of this and then start to address the problems based on that.

SIV: Mary Ellen, can I ask you to step back in on this point? Do you share John's view that we have to have the larger conversation about how much surveillance we'll accept or do you think we could actually make some progress through implementation of technologically-based use restrictions?

MEC: There are some privacy-enhancing technologies and there is some ability to scope that information that is being collected. John's example of the five minutes out of 12 hours is privacy-enhancing in the sense that it's only focused on those five minutes. But I think Greg is right that once the 12 hours is collected, everyone is going to say "12 hours? let's play." And so I think we've got to be conscious of both sides of those arguments.

SIV: Is there a way to write the relevant statutes so that there is a mandatory destruction requirement unless a specific trigger applies?

MEC: I candidly think that can really help a lot because if it's not there, people aren't going to play with it. Now, of course, every law enforcement person and every marketer I've ever met both say that they might need that information someday, and so you've got to have that conversation about what's an appropriate use in terms of how long you need to use it and what you need to use it for. We're all saying the same things about these kinds of unintended consequences and unintended uses. There is also other technology that you can put into it where, rather than identify every single person, we blur the faces until we ask where specific individuals were, and see if we can do it that way and kind of reverse it so that it's masking both the five minutes and the rest of the 12 hours.

SIV: John, do you want to jump back in?

JG: You know what the FBI's rule for mandatory destruction is? Seventy-five years. You know what the NSA's is? Neither do I.

SIV: There is a lot of support for the mandatory destruction idea. I want to ask one more question before I ask Adam to take us into the second case study: It seems as if we've been bouncing back and forth between the limits on the private sector and on the government. From your perspective, which of those two strikes you as the area of bigger concern going forward? Are there ways in which the considerations that you would think as a policy matter would apply to one are actually stronger in one context than the other? Should we be more worried about Big Brother or about Google? Or is that increasingly the same thing?

EC: I think that's increasingly the same thing. The point that has been made earlier is if law enforcement has access to that data so long as it's being collected, then they will seek access to that data.

SIV: So is the answer to tighten and reduce the circumstances in which those private entities are allowed to share that data?

EC: You can certainly look into questions of whether or not judicial review or what type of scrutiny would be appropriate prior to a request being made upon a private company, but I agree that we're increasingly blurred here.

RO: I think it's self-evident that we need to learn more and be more concerned about private data collection. That's where the oceans – this probably understates it – of data being created. And of course, those are then being tapped by the government. You asked implicitly what can we do? I think we very seriously need to rewrite or consider rewriting the Privacy Act to acknowl-

edge the reality that the government is outsourcing a lot of domestic intelligence, and if we like that as a society then that's fine, let's codify that. But if we don't, or if we feel like it needs some checks, then we need to put those into place right now. It's a fiction that there is any control on that.

SIV: John?

JG: There is a company called Vigilant Video that basically runs automated license plate reader capture devices, and just drives around and has fixed points and they sell that data to law enforcement and it's where your car goes, it's perfectly public information and law enforcement is using that to supplement their own license plate data.[10] How do you stop that? What is the line that you draw? And this isn't the government necessarily going to them, this is the company that started it: they said "great, we can collect all this data and use it," and now they are selling it to the government, they are pushing it towards the government. How do you address that, how do you stop that?

SIV: Do you not think that you could stop it by barring the government from buying the data?

JG: You could, but I see it as being very difficult to get that enacted legislatively. Basically, you would be going to the government and saying put this company out of business.

SIV: So, Beth, let me ask you the last question before we turn it over to Adam for the next case study.

EC: Lucky me.

SIV: John said it's not that it's legally possible, but that nothing realistic would be politically possible. Where are the politics of this? It seems like this conversation happens every 18 months or so, and everyone throws up their arms for a couple of days, and then people go back about their business – and no meaningful reform takes place. What do you see as being necessary for there to actually be reform in this field?

EC: My assessment of the political dynamic is slightly different because I do think that when you have technological changes or you have law enforcement seeking access to different repositories of data it does spark conversation – particularly if you need an affirmative grant of authority to get it. So what you see up on the Hill are a lot of discussions about how to deal with new technologies. And these are serious and candid discussions, and I think the Hill tends to move in the direction of allowing the authority, but, for example, accompanied by IG reports or sunsets or other types of oversight enhancements. I don't think there is a blank check for law enforcement and I think if you ask the FBI they would agree.

SIV: John and Mark and then we'll segue.

JG: Just one quick point: I spent ten years on the Hill in the Senate before coming to Palantir, and there is a maxim on the Hill when dealing with anything

10. CarDetector Mobile ANPR/ALPR, VIGILANT SOLUTIONS, http://vigilantsolutions.com/products/cardetector-mobile-alpr.

in the technology space that we should be technology neutral – don't back horses, because we don't want to stifle innovation. And this approach has snowballed into one in which we don't even want to talk about the technology or we don't necessarily think we need to learn about it. And I think it's time for challenging that notion because I think it's a mistake. I think decisions are being made in Congress where they don't understand the technology and they are actually making decisions based on their conception of technologies that they have taken in through an osmosis from watching movies and popular society. They are making rules that have in the back of their minds something that is ten years old. I think you have to break through that mindset, and they have to understand the technology, they have to understand how it works and what's out there and they need to make law and policy that leaves room for innovation and doesn't necessary back horses. I don't think they are in a position to do that right now, and I don't think the way they approach technology questions puts them in a good spot to actually do that anytime soon.

RO: Just a quick thought: In terms of change, I tend to view all of this stuff very much like the environmental movement back in 1960 or thereabouts. When I was born, people laughed at the idea that we should be concerned about curbing industry or getting in the way of a good time on the economy because cleaning up the rivers, the air, trash, litter, all that stuff was considered very secondary to economic growth. It was only when middle class moms and dads on the left and on the right embraced the idea of recycling and so on, it took 40 years for that to become common place. I think it may take as long for this stuff to really sink in and people to understand it and the pressure on Congress and other parts of our society will be great enough where a change occurs.

SIV: Bob, do you think there are things that people in this room who share your views can do to accelerate or at least put pressure on that development?

RO: Whenever possible, get out of the sort of the super micro of the now discussions about what's legal or what's happening on the Hill and keep trying to go back to fundamentals about people's place in society and the roles and autonomy that we expect.

SIV: Mary Ellen, you wanted to jump in?

MEC: The one point I want to make is following up on Beth's and John's point on Congress. Beth mentioned the IG but she didn't mention Congress and I think that's worthwhile to note that another of the abilities to curb this use or have oversight of this use is through Congress. But I do not believe that Congress is functioning as an oversight body when it involves these issues, but is functioning as an oversight body for intelligence, for law enforcement and for collection in general and I think that is part of our conundrum here.

EC: Sunsetting I do think is part of Congress's attempt to do oversight, and I think IG reports that have to be provided to the Hill do provide an opportunity for Congress to attempt to do oversight, whether they understand what they are getting or the implications of it is a completely different question but I think Congress does attempt to do oversight.

MEC: I disagree with you on that one.

SIV: Well reasonable minds can disagree.

MEC: Yeah, we agree on everything else.

SIV: Marc, why don't you wind this up?

MR: I want to give two answers to the case study in broad terms and both of them have an historical precedent. The first one is that these programs are typically deployed by funding from the Department of Homeland Security and the federal agency could establish best practices and say that any municipality that wants to deploy one of these systems has to meet the following eight or ten requirements and the agency could hold workshops, meet with experts, consult with Congress, figure out what those standards are and actually make them a condition of the grants to the municipalities. In fact, DHS did something very similar in 2007 with the initial deployment of CCTV.[11] We favored their standards – in fact, we got upset with the agency when they failed to hold the municipalities to the standards that they had established and went ahead and funded them. But here is a second approach that EPIC, my organization, has taken a real interest in over the last few years. And that is that you can petition the agency to establish privacy standards and in fact that is what we did with the airport body scanners and this is the reason you don't have the nude body scanners in U.S. airports anymore because we sued the Department of Homeland Security when they failed to act on our petition and they had to eventually establish privacy standards.[12] EPIC did the same thing recently by the way with the FAA and drones who just announced a privacy rule-making, and I think you are going to read tomorrow about another exercise we're pursuing. I appreciate everybody's comments but I do think in looking at these different scenarios it is important to get concrete. There are a lot of generalities about how Washington responds to new civil liberties challenges but sometimes if you get into the details you know you can understand the problem, respect all the sides to the debate and then come up with a workable solution that could have some lasting impact.

SIV: Thanks Marc. So our next step we have on the back of the handouts that you all received at lunch is another case study[13] which we'll spend a little less time talking about since we teed up a lot of these issues in the first conversation. We're going to spend a little time going through this one before turning to audience question. Adam, do you want to walk us through the second case study really quickly?

AI: I know that some of the members of this panel and expect that many members of this panel some are somewhat familiar with passenger name record

11. DEP'T OF HOMELAND SEC., CCTV: DEVELOPING PRIVACY BEST PRACTICES (2007), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf.

12. Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., 653 F.3d 1 (D.C. Cir. 2011) (holding that the TSA impermissibly failed to undertake full notice and comment rulemaking on its use of airport body scanners).

13. The second case study is reproduced as Appendix II to this Transcript.

(PNR) information. But for those in the audience who aren't, airlines as part of the reservations process collect certain data on passengers and for 20 years or so the U.S. government and other governments have looked at that data to inform the border inspection process and risk assessment process. After September 11th, the provision of that data became mandatory in this country – as it is now in several other countries. But because it basically involves the bulk transfer of data on innocent persons to the government, it's been controversial, particularly in Europe where obviously a lot of traffic that comes to the United States comes from. It's kind of ironic sitting here right now because the U.S.-EU PNR agreements now have been not only agreed to but ratified by Parliament in Europe itself, which is now on the verge literally of establishing its own entry/exit system and its own process for processing PNR. There is a draft PNR directive that is theoretically being vetted by the Parliament this year. So people who come across the border have got to be inspected anyway, and the idea behind using this data is that it informs the inspections process and makes it more risk-based.

One of the challenges is that given the nature of global travel you are limited in the scope of what it is you see if you are only looking at the if you will the last itinerary before someone arrives at your country and so the idea around this case study is that there is an opportunity for the nefarious traveler – the malicious actor – that starts a journey in Thailand and stops in Singapore and a week later commences travel to the United States to engage in a multinational advance travel information data exchange program. The question is, given the difficulties of establishing sharing between the U.S. and the European Union, how much do you think about establishing this kind of a concept on a multilateral basis? Given the disconnect between how jurisdictions are set up and the globalized nature of travel, I thought this study might be helpful to get some discussion going on how you think about privacy constraints in a multilateral context.

SIV: That's great. On the multilateral side, it seems like there are pressures in both directions, right? That is to say, there is some pressure to do whatever we can to cooperate with our friends and to be able to get information that they could share with us to bolster our ability to conduct these kinds of investigations. Is there any concern about sort of pressure to sort of lower our standards, that many of the countries with whom we would be sharing this data don't have the same kinds of statutory and constitutional privacy protections that we've come to take as well-accepted? How might that work in this scenario? I don't know if anyone wants to start there specifically, but Adam I'll pick on you.

AI: I think this question is going to come up and it's probably going to come up in Europe regardless of whether anything ever happens with this case study, because there are absolutely parts of the world right now that are looking at using PNR data for circumstances where there is direct air service from Europe. So it would be interesting to see how that goes. I do think this gets to the

question of data ownership in making sure that the entity that actually owns the data maintains control over it.

SIV: Mary Ellen?

MEC: And I think Adam is right that this scenario may come up because the first question I would say is does each country have the authority first to collect the information? The U.S. has a statute that requires the submission of this data before a plane arrives.[14] The second question is whether the country has the domestic legal authority to share it – and if they have the authority to share it, they should make it an affirmative statement. We have our system of records which are Byzantine and horrible to read and very archaic, but there is at least the ability to make some sort of statement if there is going to be that sharing. The negative side is that then you do have sort of you have six countries who have all kind of dumped their data in a pool you now have more visibility into where the person has traveled. Is that protected information? I can make both sides of the argument on that. It goes to what are you doing with the information. If you are looking for these pattern-based activities where you have no basis – if you go to Thailand and then switch in Singapore and have a new PNR that's indicative of something – then that should have higher privacy and civil liberties protections because it's not subject-based. We heard the GC of the NSA say he has individualized suspicion on types of stuff. Here it's not; it starts with non-threat based information, then you extrapolate. The more that goes into the big pool, the more protections you need to have.

SIV: Greg, let me put this to you. Is there any argument in this context that one of the big distinctions from our first case study where you have private citizens walking around on the street is that, here, you have a situation where individuals are presumably at least implicitly consenting to the collection of this information, perhaps even *expressly* consenting to the collection of this information? I suspect you have a problem with the premise of that question.

GN: We keep talking about consent. When I have to go to a conference in California, are you telling me that I consented to the collection and the sharing with these foreign governments – that I know nothing about – of the fact that I went to California and all my other traveling? There is no consent there.

MEC: I will distinguish a little bit. In Adam's hypothetical, it's foreign travel, it's not domestic travel. So it's border-crossing types of information.

AI: Yes.

GN: But that makes my point even more strongly. When I'm going to Italy, I have no real good way to get there but to fly.

SIV: Cruise ships are out this time of year.

GN: You saw what happened with those. So I just think to call it consensual is a myth. We should just not even talk about whether there is consent.

SIV: Bob, do you want to pick up on that?

---

14. *See* 49 U.S.C. § 44909(c) (2012); 19 C.F.R. § 122.49d.

RO: Again, I don't want to get too primary colors on everybody, but it doesn't make sense not to collect the information and it doesn't make sense in a theoretical way not to use it to reduce risk

GN: They got to you didn't they?

RO: He's been saying that for years. But I don't think it should be allowed until we do the hard work and pay the money that it takes to ensure that if it's misused or abused, that people suffer consequences for it. It's the same balancing act; it's sort of binary – if you don't have those rules in place, you don't use it. If you have the rules in place you try to enforce them. Are there going to be abuses, yes, but presumably your system is going to be good enough. But the idea that we are not going to use new technology and techniques just because of the potential problem they pose is ridiculous, and at the same time using it without spending the money and taking the time and the hard thought to make sure that the abuses are minimized is also ridiculous.

SIV: Marc, doesn't the introduction of the cross-border element at least raise a different specter than we saw in the first case study?

MR: Oh I agree, it's a great case study partly because some of the challenges in the big data field have become global as governments are trying to coordinate responses and that in many respects seems quite rational. At the same time, this is the privacy issue that set off a wildfire in Europe after 9/11 because, when the European Council on behalf of the European governments entered into an agreement with the U.S. government for this data disclosure, the European Parliament said "you actually are violating our rights under the European Data Protection Directive." They sued the Council in the European Court of Justice, and actually on a technical ground.[15] It was not a substantive determination but you have to understand how strongly people in Europe felt about this. Imagine Congress suing the President and going to the Supreme Court over the disclosure of passenger data. Now here is the problem. The problem is that whereas the Europeans would say privacy obligations attach in our record system regardless as to who the data subject is, in the U.S. we actually draw a very sharp distinction in the Privacy Act.[16] We say you are either a U.S. citizen or you are a lawful permanent resident and if you are neither then you have no legal rights and so the objection that is raised on the European side as you are gathering all this data we have no rights, we object to that and our response tends to be well if you want to land your planes here you are going to have to give us the data first. I don't think that's a satisfying policy resolution so there is going to have to be another approach to try to over the long term answer this question: how do we acquire and use data and still provide legal protections in a trans-border data context?

---

15. Joined Cases C-317/04 & C-318-04, Eur. Parliament v. Council of the Eur. Union and Comm'n of the Eur. Cmtys., 2006 E.C.R. I-4721.

16. 5 U.S.C. § 552a(a)(2) (2006) ("the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence.").

SIV: Let me ask a question to which I think I know the answer: Is there any possibility that in this scenario the mandatory destruction possibility that we contemplated in the first scenario could work better?

MR: That's been one of the key issues in this particular debate going back to the original agreement, and it had to do with a number of categories of data that were kept and the duration of the data – how long it was being kept, as well. People argued in the negotiations very strongly over this. I just want to throw something else on the table which I think Adam's case study suggested as well which to me is fascinating. Again, this is another topic where there is a lot of probabilistic analysis going on. In other words, it's one thing if you have a watch list and you say we have a warrant for this person or we have them on a list and we don't want them to enter the country, and if they are entering the country we're going to intercede. That happens, but most of the border security in this country is actually done by assigning a likelihood to whether a particular container for example is likely to contain something that poses a threat to the nation's security. And that technique has also been proposed and applied in some circumstances to people entering the country. "We don't have them on a list, but let's look at these seven or eight factors, maybe we should look a little more closely at that person." That discussion also comes up with PNR data. And by the way, your premise on the question was a little backwards. You were saying there are these countries around the world that don't have the same great rules we have about privacy. Really? In the PNR debate we were the lowest common denominator.

SIV: John, can I ask you to jump in here? On the technological perspective, is there a way in which the pure passenger data side of this scenario raises an easier variation than the complex facial recognition conversation we were having earlier with regard to the first hypothetical? Do you think the technology actually cashes out a little bit easier here because it's straight data collection?

JG: If you got this panel in a room, and we designed the perfect data exchange system, I think it's highly possible that you could build that system with the technology we have today. There is technology to build federated systems where data is used but not centralized, is not exchanged with anyone or the original data owners don't lose control. There is possibly very granular access controls, there's a possibility to have very powerful audit logging capabilities, and I think you could use all this to support policy – it has to go with policy to address so many of the sharing and processing questions. Now the collection questions – how the data gets in there – is out of that purview, but on the processing and sharing questions, I think you could resolve most of this. So why don't we build it? Because to actually manage it requires a lot of time and resources by some data steward and that is where a lot of data systems in existence today fall down. If you go to a lot of local law enforcement agencies, the privacy officer is a sergeant – is somebody that drew the short straw at a staff meeting and is now responsible for the privacy maintenance of whatever system they have, and this could be millions of records even in very small law

enforcement systems. So you need to devote resources and personnel to actively managing your data, from setting the access controls to reviewing the audit logs, and pushing and pulling information back and forth. And that is where I think it starts to fall down. But I think the technology is there to build the system to support the human generated policy. I don't think it's in the realm of possibility even in the next 20 years to build some sort of automated system that is going to do all that and I think chasing that is a fantasy and I think it's a mistake. You have to have a person making these decisions because of all the contextual questions that come up. I think it's very possible to build. The question is whoever is in charge of this, are they going to put the resources into actually managing it?

SIV: John, you say not in the next 20 years. Mary Ellen, can you give us a sense of where we are today and what you see as the biggest pitfalls with the current status?

MEC: Sure. I was part of the most recent negotiation with the EU—I think there were four, and Beth was involved in the second. The standards for the U.S. collection of PNR right now in terms of retention are that the data will be collected and this is worldwide, the EU has the standard but the U.S. is applying it worldwide, information will be collected and after six months all personally identifiable fields will be masked. They will be only unmasked for a law enforcement or international security purpose for five years, and then if it is a national security purpose it is going to have particularized standards and individual suspicion—and will still go in another five years. So the idea is consistent with what John was talking about in the context of the the earlier hypothetical, about trying to minimize the exposure on the non-particularized suspicion for the traveling public. So just FYI in terms of where we are in the U.S.

SIV: Let me ask a different version of the same question. We've been talking about the difficulties with policy reforms in this area, we've been talking about the technological challenges not from a design perspective, John, but from the perspective of who is actually going to sit at the machine and do the work. Have we been leaving off a possibility that another institution might reassert itself in this conversation, *i.e.*, the courts? Is it possible that in the light of little movement on the policy front from Congress, from private industry, from everybody, that the courts might actually use the Fourth Amendment to ratchet back up what we haven't been able to accomplish through lesser means? Haven't we seen hints of this in the *Jones* case, and in the oral arguments earlier this week in *Maryland* v. *King*?

EC: If I had to guess, the Supreme Court would be much more likely to intercede on the first hypothetical than the second hypothetical. Particularly when you are talking about transnational and border situations, the Supreme Court and most courts have shown a high level of comfort with a lot of inspection, so I think if you are going to see movement it's going to be in the first one rather than the second.

SIV: So while we're there, is there a scenario where you think that could be possible in the first case study?

EC: I do think that there is a possibility. Some of the things that Bob was talking about calls to mind the idea that conventional expectations of privacy now seem to be a quaint anachronism at this point. So how do we move the Court into a more realistic assessment of what we should expect when we go into public spaces and what law enforcement can do? Can it be targeted? Can it be continuous? What can you be looking for? Are you only keeping the alerts or are you keeping the other 11 hours and 55 minutes of data and then what are you doing with it? I do think there is a possibility that the Court would intervene on that probably prior to Congress.

SIV: Indeed, part of what helped lead to FISA was the Supreme Court sort of stepping in when it did in the *Keith* case,[17] and then the Church committee. Marc?

MR: The flip side of global data flows is that you are now talking about more legal institutions than just those that exist in the United States. The PNR episode triggered a response from the European political and judicial institutions. Over the years, I've noticed the growing prominence of the European Court of Human Rights with its Article 8 jurisprudence under the European Convention on Human Rights. This is similar to our Fourth Amendment, but with more detail. And that court has reached out many areas – biometric identification, for example, and workplace surveillance – and announced new rights to privacy. Our Court, by comparison, is not doing as much. But a lot of people do get the sense after *Jones* and even after the *Maryland* argument this week that the Court is very interested. So I would never foreclose that possibility. But I would say that when you think about data flows in a global environment, then a lot of other institutions actually become significant players. In particular, in Europe, it is the European Court of Human Rights.

SIV: In other words, we should put our faith in having our privacy protected by Strasburg.

MR: Basically yes.

SIV: Greg?

GN: One more scenario to which one could look for where the Court might go with the *Jones* reasoning is in cell phone location tracking. There are some cases that are bubbling up through the circuit courts that might result in a split that would force the Court to reach a decision about whether law enforcement can track your location over time based on the location of your cell phone.[18] Looking at what the Justices wrote in the concurrences in *Jones*, I think there might be five votes to say that requires a warrant.

SIV: John, and then Bob.

---

17. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297 (1972).

18. *See, e.g.*, *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).

JG: One direction that might be interesting to see if this develops legislatively or in the courts would be more process – more rules at the point of analysis versus collection. You have to show some reasonable suspicion or probable cause in order to analyze the data in a certain way or match it with other certain data sets in which you are pulling information out. Now, how you get there judicially is complex. But I think *Jones* sets that up in that they are recognizing that there is hidden data within data. You can infer or derive things from bulk information that people maybe are showing publicly, but they aren't expecting that they showed other information. For example, I know that people can see where my car goes, but did I realize that if someone pieces together where my car goes for a whole month they can figure out if I'm cheating on my spouse, what religion I am, or if I have a particular political affiliation? And I can see the Court saying that there is some expectation of privacy – that the government is not going to be able to apply really sophisticated computer analysis to pull information that you didn't consciously expose out of data.

SIV: So the argument is that the mosaic theory actually might show up in the other direction as a new way to reinvigorate the Fourth Amendment in this context? Bob?

RO: Regarding the cell phone tracking, which I think is fascinating, I don't know how many people here recognize that there is a company in New York that collects the data about every time your cell phone pings. I don't even know how much data it is, but it's a fascinating unexplored pool of data that never existed before. They claim that it is anonymized, but it takes two minutes of thinking to realize that wherever that cell phone ends up for eight hours in the middle of the night is the geo-coordinates of the owner. To me, if there are any journalists in here, that's a fabulous thing to pursue that I've not read about.

SIV: Aren't you a journalist?

RO: Yeah, I've got other assignments. But the other thing that John mentioned – and again I'm going to do the non-lawyer thing here – so many of the problems that we're trying to confront in the data revolution whether it's privacy, cybersecurity and so on, are directly related to a very simple idea, which is the government and companies are not paying the full cost of doing business. It's an externality of sorts, like pollution or identity theft. If we could figure out a way through law and policy to get entities to pay the full cost of doing business, there is going to be a lot of the stuff that is just going to disappear because it's currently a freebie, for example, for law enforcement in effect to ride piggyback on this private data. I just think that's a very insightful idea.

SIV: Greg?

GN: Just to add a little bit to those comments and to John's thoughts and to Raj's speech from earlier, one thing we have to think about is in the age of big data what aspects or principles of fair information practice do we need to stress more and maybe bolster? And just to take an initial shot at that, I think they are redress, oversight, and accountability because we are going to lose a lot on the

other side. And then there is another one, due process, meaning what happens to you after intelligence is drawn out of that data. Senator Wyden had a very interesting amendment[19] at committee consideration of the reauthorization of the FISA Amendments Act – the act that allows NSA to target people abroad without individualized suspicion. And what he said was what I'm worried about is you using that data to find what U.S. persons are doing to get their information. What he said was, I want you to have a warrant to search through that data when the target of that search is a U.S. person. Now he didn't pick up a lot of votes at committee, and he didn't offer it on the floor, but I think that concept is one that we need to think a little bit more about – on due process ground.

SIV: The Constitution Project has actually suggested exactly that much – that one way to think about this problem is not as a front-end Fourth Amendment and privacy problem, but as a back-end problem: once you have the data, you still need individualized suspicion to actually parse it for specific content. Marc?

MR: So I want to pick up on that and share my own personal campaign to make algorithms transparent. We talk a lot about the importance of transparency in the privacy world, and invariably when you make a request from a company for information where you have a transparency right you get back your name, your home address, and your telephone number which for most of us is not particularly useful. That's really not the point of transparency in privacy laws. The point of transparency in privacy laws is to understand how the data is used and how the automated decision impacts the individual. So when we think about online advertising, for example, or we think about who gets pulled aside in security lines, or we think about determinations regarding credit, the real key is to understand what is the basis of that determination, which is a matter of procedural fairness. This gets very, very difficult, because any organization in possession of a lot of data that is making determinations about people over which some people might actually hold that it was wrong – the data was old, you've got the wrong person, you shouldn't have done that to me – are very reluctant to reveal the basis of the determination. But today, particularly in our world of big data, this is the hard problem is forcing organizations to be more transparent about those rules.

SIV: Bob, I want to get to you in one second. Before I do, we're going to turn to audience questions in a second. I want to warn the panel first, though, that I am about to ask you so what you want to see happen in the next five years. Bob?

RO: I just wanted to underscore the very, very important message that Mark just delivered. I don't know if you all have a copy of this on your table, but here is [a graphic] I created for some of my colleagues to spell out why this stuff mattered. This is the data trail that we left behind in 1973 when the Privacy Act

19. S. REP NO. 112-174, at 12 (2012), *available at* http://www.intelligence.senate.gov/pdfs112th/112174.pdf.

was passed. This is the data trail now, and you'll see some colors in there and those colors relate to the algorithms. And this is the data trail 40 years hence. And if you see, it's just black – we're going to be leaving so much data behind us that it's just dense. But it becomes beside the point because these links that are the algorithms are going to become so good that they allow the corporations or the government to do predictive analysis. And that's the point of this – a simple illustration of the power and importance of algorithms going forward not just the data.

SIV: Adam, you were gracious enough to contribute this case study, so let me start my last question of the panel with you: We've made some progress in getting to what the big issues are, and we've identified some of the key obstacles. What, to you, are the most important things you'd like to see happen in the next five years in this field so that, when we all come back for the reunion tour we're not having the exact same conversation?

AI: A couple of thoughts. I think there is actually a connection between these two case studies. And the connection is this: You can have a privacy related concern – a civil liberties lawyer concern about whether this data should be collected in the first place. But you can also have a concern about the accuracy, the underlying accuracy of this, and the right decisions being made on the basis of right information. One of the challenges we have with text-based data right now is the challenge of identity resolution – does this actually mean what you think it means. And so what you are going to see over the next five years is a huge expansion. So privacy by design in the development of those systems is critical. With respect to this case study I think that in the second case study, the issue that I was trying to get at with the PNR is really a question of how do you do privacy oriented multilateral information sharing? Honestly, you could move API and PNR and governance, and think about cybersecurity. And you could think about signatures and heuristics and how it is that we're going to keep our IT systems safe when the information about threat is as distributed as it is. Again, the key is the importance of thinking about giving the data owner some control over how the data is managed in multilateral contexts, and allowing the data owner to differentiate. How do you put the right audit mechanisms in place such that you could after the fact have some transparency with what people did with it and maybe anonymized as well?

SIV: John, can I have you pick up from there?

JG: Where are we in five years or where would I like to see us? I can think from a technological perspective but more from just an advocacy perspective, I consider myself an advocate. I've been doing these conferences for the last 10-12 years and I think they are great, I think they are full of fascinating ideas – really intelligent people making great points to each other that they all agree with. And as advocates we're getting our asses kicked. We lose just about every fight that we take on, and we certainly have very few things come out as a win. The closest thing I've been involved with that was a win was I spent seven

years fighting REAL ID – a national ID standards project in Congress.[20] And we eventually sort of won because DHS just kind of gave up on it and so waived most of the requirements. We never actually had a real victory, and so what I think we need to do in the next five years as a community on these issues is figure out a new approach. We're losing in the courts. We have a Democratic President who everybody sort of expected would review things like the PATRIOT Act and all of the various Homeland Security mechanisms. Instead, he has fought aggressively to protect them. I commend to you *Taking Liberties* by the President of the ACLU,[21] which I read through clenched teeth on a vacation. In it, you see examples of this problem. So if we are going to convince people to change, and it's got to be the courts, it's got to be the government, and it's got to be the public, we've got to take a new approach. We've got to take a new strategy. It starts with trying to break people of the idea that government can provide you with 100 percent security. This is the rhetoric right now. If something happens we will make sure it never happens again. It's what the public demands; it's what politicians like to say; and it's what fuels this whole meme in which privacy arguments can be defeated by anecdote because all you've got to do is find one time in your entire data set where you found something valuable that would have prevented another 9/11 and the privacy argument loses right away. It's really hard to have a public relations campaign that is along the lines of "sorry, you may die." It's not like you're going to win people over with that. I don't know how you do that, but one of the things is that we've got to start preaching to the choir at these kinds of events, and start thinking about how do you actually effect real change in this space. And to do that you've got to come up with a new strategy.

SIV: I will now forever remember this panel for the "sorry, you may die" retort. Beth, can I turn to you?

EC: Picking up on some of the themes here in terms of accountability, I would look at it slightly differently. We need to develop metrics and ways of assessing whether or not the information that was asked for – whatever authority it was that was requested it – has it truly borne the promise that folks came up to the Hill or wherever they went to ask for it? Has it worked out as it was represented to work out? Has it really performed the function – has it been used for the uses for which it was originally sold? I do view it as an accountability issue – it is okay to ask whether it is on the front end or the back end, but ultimately is this really going to work, and is it worth it?

SIV: Mary Ellen?

MEC: With regard to accountability and oversight, I look forward to the full completion of the Privacy and Civil Liberties Oversight Board.[22] I think that's actually going to help the dialogue a lot within the federal government. My

20. REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 302 (2005).
21. SUSAN HERMAN, TAKING LIBERTIES (2011).
22. *About Us,* PCLOB, http://www.pclob.gov/about-us.

point on congressional oversight, just to clarify, is that I don't think that they are asking the types of questions that Beth was talking about. I think they are engaging in oversight in many ways – and I've had to testify to prove that – but they are not asking these ex ante and ex post questions. I think that is an important dialogue, and so hopefully having the PCLOB in the mix will help kind of tease these issues out because in five years there is going to be more holistic, comprehensive, non-threat, non-particularized suspicion-based collection. What I hope will happen is that we actually use privacy by design – that you think about this and you define the usage, you define the collection, define the data destruction if need be ahead of time, so we're not caught flatfooted when somebody wants to access information whether it's private or public in the future.

SIV: Marc?

MR: I've been teaching privacy law for a long time, and sometimes I think it's maybe more the history of privacy law and other days I feel like it's the archeology of privacy law. The truth is, you go back to the passage of the Privacy Act in 1974 and the events that led up to that, and there was a tremendous national focus and public debate about the emergence of databases and databanks in the U.S., and automated processing.[23] Many of the same discussions we're having now about big data are actually similar to those debates. I will say today by comparison there is probably a greater sense of the democratization of computers, because now we all have access. But this is my answer to your question: A lot was done in that period of time to try to create legal safeguards, oversights, and ways of talking about these issues that are enormously valuable today. And we need to rediscover some of those lessons. We need to understand why the Privacy Act put in place the prohibitions on profiling that it did, why for example it's so important to give people access to information about them so they can make meaningful decisions. All of that can be found in this history but you have to do some digging. So I'm hoping over the next few years for seminars on the Privacy Act and FISA and a few other of those favorite federal statutes.

SIV: Fair enough. Bob?

RO: Just as a side remark, I would like to point out I believe congressional oversight is a profound travesty – I would use the word pathetic. And we're going through a terrible time and they need to improve on that so I appreciate the gracious way you put it. And I think that once again, Marc hit on something that is very important and I'll just put it in different words. Back in the early 70s, the middle class – and I'll use this term advisably – was radicalized, and they realized that there were a lot of bad things that were going on, there were massive abuses of official power, and it all came together in a bunch of different ways. But one of the ways it came together was the Privacy Act, people said there needs to be a check on government power. I think in the next five, ten or

23. History of the Privacy Act of 1974, EPIC, http://epic.org/privacy/1974act/.

fifteen years, the bulk of our society needs to understand this stuff and become very, very assertive about putting a check on the government power and on the security industrial complex that is taking advantage of the very laissez faire oversight and the lax application of the rules and such.

SIV: Thank you. Greg?

GN: If we're doing our jobs well in the next five years, we will learn how to use privacy debacles to turn into new privacy policy. I think that's a big challenge. I think there are a lot of debacles out there, and we just haven't figured out a good way to personalize them so that the average middle class person says "oh my gosh, something needs to be done right away!" The other thing I think is that, if we're doing our jobs well, we will do better in figuring out how to reimagine some of the principles of fair information practices to make them more relevant and more alive in the age of big data. We're going to be doing some of that thinking at CDT and we'll be drawing out some of the good thinkers in this room to help do that.

SIV: Great. We've got about 25 minutes for questions from the audience. I just have two requests of the audience. One, bear with me because I have to come to you with the microphone in my Phil Donahue style. And two, please try to phrase your comments in the form of a question.

Question: Thank you. My question is, essentially, do you think it would be helpful to rephrase or reimagine our way of looking at privacy to start by instead of what do we do with PII to instead look at what causes us to identify you positively, and I'm thinking in the case of these hypotheticals I may take a picture of you as you walk down the street and I may check to make sure you are not on Watson's warrant list or things like that, but I don't identify you unless there is a reason, *i.e.*, you've committed a crime, you're being sought. Do you think it's helpful if we shift our thinking instead from how do we control what we collect to what do we do with it instead?

MEC: I think that inevitably with this significant collection of information defining the use is going to be more important than collection itself, so yeah, I think that can be part of the discussion I don't know if it's reimagining privacy, but I think it's reconsidering again the fair information practice principles as Greg said in this era of big data.

GN: I think it solves some of your privacy problems, but what if, instead of a sort of semi-concealed CCTV camera, it was a cop with a camera. So you can see that there is a cop taking pictures of you as you go, you are going to curtail your action, you're going to respond to that, and it doesn't matter if it turns out that the cop isn't actually trying to identify you or use your information, the negative effect of the surveillance still happens. So it gets to some of the issues, it doesn't get to all.

Question: Fixed surveillance cameras are ubiquitous in London and in large parts of UK. So if you folks have any comments about how effective they have been and particularly how effective that CCTV is, and that CCTV is down on the corner – and then also on the first hypothetical, your reactions on whether

the database used for matching was a driver's license database or a mugshot database?

JG: Greg just volunteering for the second one. Actually I'm going to volunteer for the first one because I just had done some work on this. There are a lot of studies from the home office and from various UK both NGOs and government agencies that say it hasn't been that effective or it's been minimally effective or it hasn't done what it was supposed to do. That they put them in for in certain reasons to find serious crimes, but they ended up using it to find petty crime or they worried that crime was just pushed off into the streets where the cameras didn't exist. So I think there is a lot of data that it at best says that the London CCTV experience produced mixed results, or that, at worse, it didn't work at all. I commend Jeff Rosen's book, *The Naked Crowd*, in which he talks about this extensively and really well.[24]

AI: John, I would just add that I think it depends on what the purpose is. If the purpose if prevention, I think maybe the analysis is different than if we're talking about moving right into a response context. Because if you have the ability for instance to link you know a 911 call with CCTV image and drill into that pretty quickly – and I have no idea whether they can do that in London or not – you could have some pretty strong response enhancements there.

SIV: Greg, were you going to take the second part?

GN: No. But what I was going to do was say that we need to be a little more concerned not about just the fixed cameras but also the ones that are going to be mobile and up in the sky and very effective at peering down at us from drones.

MR: On that point, we at EPIC obtained some very interesting documents from the Customs and Border Protection agency in the last week which I think you are going to be reading about very soon in terms of what those drones can do.[25]

JG: I would like to point out the London experiment does serve as a great example of how technology manufacturers – and I'm not being ironic here – are very good at selling something with what seems to be an obvious claim that it's going to reduce crime, when the reality is that they are really not checking and the outcomes are not nearly so clear. So we have lots of stuff being sold to the U.S. government where there are claims for it that aren't backed up by any data or any studies or anything.

Question: I'm curious if there is any current discussion going on about giving the people who are producing this information control over it – if so much of this ocean of data is coming from my cell phone or your mobile device,

---

24. JEFFREY ROSEN, THE NAKED CROWD (2005).

25. EPIC released these records on February 28, 2013, one day after the symposium. *EPIC FOIA – US Drones Intercept Electronic Communications and Identify Human Targets*, EPIC (Feb. 28, 2013), http://epic.org/2013/02/epic-foia–us-drones-intercep.html. For more information on the contents, *see* Declan McCullagh, *DHS built domestic surveillance tech into Predator drones*, CNET (Mar. 2, 2013), http://news.cnet.com/8301-13578_3-57572207-38/dhs-built-domestic-surveillance-tech-into-predator-drones/.

is there any discussion about allowing me to select what I'm sharing with everyone?

GN: It's a very important question because, if you think about it for a moment, it's actually the core of the right of privacy that you do have some control over your personal information held by others. What most people do is they think that the legal right mirrors your physical capacity, so it's like if it's under a lock and key then it's private. But of course it's private in that sense only because of a physical control. So the question that the law tries to answer is that, outside of the physical control, what kind of rights do we give people to their information when, for example, they pick up a telephone and call someone else, or when they disclose sensitive medical data to their doctor, or when they reveal financial information to a bank? All of modern privacy law is actually about establishing some degree of control over that information held by third parties. Now of course there are competing claims, Law enforcement can say this fellow is a suspect; or someone can be suing the person and say we need to get access to the records. But I think your question is actually what is *privacy* – it's about controlling your information.

MEC: I would also note that, particularly when you are talking about the private sector, there are market-based solutions, there is market-based competition. I think about the very highly successful recent Bing commercials – you are getting "scroogled" – which is explaining to people what Google is doing with your g-mail, and giving that information to incentive users to choose not to use g-mail. Individuals going with providers that are not required to retain certain types of data, and don't, and voting with your feet for a provider that chooses not to retain it, is one market-based solution.

JG: I would say another interesting sort of technological line from that is figuring out how to make your preferences persist. Your data is necessarily shared – somebody is going to end up having some sort of physical control over it, so it's hard to tether it all the way back to you at all times. But I think there are interesting lines that you could pursue to try to figure out technological ways to allow our preferences to persist over time. One of the things that Palantir does, for example, with some of our work is that we incorporate DRM digital rights management technology into some of the documents that we use, and that prevents cutting and pasting or printing or certain things on different systems. So developing that from a technological perspective would be interesting in terms of giving individuals more control over their data, at least over time.

Question: A lot of the focus has been on government retention of data and government use of data, but I think maybe as the last question alluded to, there is also a huge concern about private companies holding on to data independent of what they may do in interaction with the government. It seems like consumers and users are at a significant disadvantage if they have to constantly update their preferences in data usage policies and their own preferences in their social media networks and what not. What do you think about some discussions that have gone on in the European Union about having the default setting being a

right to be forgotten? Is this (1) technologically feasible; and (2) would this be legally problematic or could this be somehow legally implemented?

SIV: Who would like to start with that?

RO: First of all, a lot of the services that we get are based on data being shared and maintained by these companies, so it would be very hard for a cell phone company – to take an obvious example – to get rid of your data. The same for our preferences when we are online and for the services that we use. John will know better than I, but I'm pretty sure it's possible to do what you are saying, but it's highly unlikely – and the companies are very, very effective at lobbying against it if it even comes close to that.

GN: This concept, which has been almost ridiculed in the United States is actually not at all so unfamiliar to the legal system here which you know we have concepts of expungement in juvenile records and other ways in which we protect disclosure of information. In the copyright context, there is notice and takedown all the time to search companies when the concern is copyright infringement as opposed to privacy violation. But the other thing to say on this point is that I think there are two ways to think about the right to be forgotten which may make it a little bit easier as we talk about solutions. One is in the physical sense, can we actually remove the data. Now that can be a hard problem. It's one thing to go to Facebook and say I'm no longer a Facebook user, I would like you to delete my account, which I think is a reasonable request. But to ask Facebook to go to everyone who might have shared one of your wall posts or your photos to also remove that information, that's probably going a little too far and I don't think I would favor that. Now there is a second sense in which we think about the right to be forgotten as allowing us to create legal restrictions on the use of personal data which even though it may be accessible, we don't allow legal judgments to be based on. We do this all the time, we do this with race, we do this with gender, we do this with age, we're doing it under GINA – the Genetic Information Nondiscrimination Act – with genetic information.[26] We say there are certain characteristics about people upon which we don't think it's permissible to make a legal decision. So I think that's another way particularly in a world of enormous data that we can think about protecting certain rights even if we can't physically remove all the data.

SIV: John?

JG: Steven Bellovin, who is a computer science guy at Columbia I believe, did a paper a couple of years ago, it was presented at the Privacy Law Scholars Conference where they basically took I think it was 63 computer science graduate students and they gave them a survey and said what are your preferences for sharing certain types of data on Facebook. And then they gave them a Facebook account and set your privacy settings to reflect your preferences. Sixty-three of sixty-three computer science graduate students over-shared infor-

26. The Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (2008).

mation.[27] None of them got it right. And these are people who work with computers all the time – who have Facebook accounts and really understand this stuff. And so the interesting line that this paper took was that you could sue Facebook on a product liability claim that the product was defective, and the Facebook people loved it. But what I think is interesting about this is typically, when you are thinking about the technology to actually support these kinds of preferences in what people want, the technology doesn't work that well because it's obviously not giving people the feedback they need to understand what they are sharing. Now, some people are probably making bad decisions, some people aren't putting enough time and thought into it, that's true. But again, I think if you've got sixty-three of sixty-three computer science students who aren't able to really effectively use technology to manage their own expectations of what they are sharing, what they are doing with their data, then you've got to fundamentally reevaluate how you approach this if you want society a large to be making decisions about what they share what they don't share knowing where their data is so that they can demand it be deleted. And that's obviously really complex and that's a really tough puzzle to crack right now.

SIV: What if you did the same exercise with sixty-three privacy lawyers?

JG: Well what I took from is even more interesting – what are the chances that 50-year-old analysts at the CIA are setting their access control preferences correctly?

SIV: There is that, too.

Question: To the previous question, there is actually a very distinguished report from a bunch of European computer scientists who said the right to be forgotten is not implementable, and that was actually funded by the European Commission.[28] I actually wanted to see if it was possible to sharpen what I think is the distinction between Bob's view and everyone else on the panel. I think Bob was saying you guys are all in the weeds, and there are some larger set of questions about what would actually activate a larger number of people to actually do something. I heard Bob saying it had actually to do with creating more enforceable rights that people could actually go and have vindicated. And I feel like the rest of the panel didn't exactly agree with Bob but also let him off the hook. Maybe it's because he's a reporter and you are all scared of him, but just to kind of get you going, I have to say I often find the discussion of the difference between the U.S. and Europe to be based on a fiction about the difference – that somehow Europe cares more than the U.S. does. Europe does care a lot about privacy, but they have no idea how to enforce the laws that they put into place. We seem to let them off. Privacy advocates let them off the hook in fact encourage them in that. I think it plays into the problem that Bob is

27. *See* Michelle Madejski, Maritza Johnson, & Steven M. Bellovin, *A Study of Privacy Setting Errors in an Online Social Network*, *in* PROCEEDINGS OF 4TH IEEE INTERNATIONAL WORKSHOP ON SECURITY AND SOCIAL NETWORKING (2012).

28. PETER DRUSCHEL, MICHAEL BACKES, & RODICA TIRTEA, EUR. NETWORK & INFO. SEC. AGENCY, THE RIGHT TO BE FORGOTTEN – BETWEEN EXPECTATIONS AND PRACTICE (2012).

talking about, which is that people talk about privacy but don't actually talk about things that are real that are enforceable. The U.S. Federal Trade Commission has three or four major consent decrees against Google, Facebook, Yahoo, Twitter, and others.[29] They involve more than a billion users which means more people than are in the United States are covered by U.S. enforcement, so I'm just interested in whether the panel could maybe pick up that thread.

MR: I just want to make two brief comments. For those who don't know, this is Danny Weitzner, former deputy chief technology officer at the White House. Among Danny's many accomplishments, he helped pull together the President's Consumer Privacy Bill of Rights,[30] which we think is a very good articulation of the right to privacy and would like to see that established in law so I certainly think the U.S. is making important efforts. Trust me, no one goes to Brussels for the weather – that's not the reason for traveling overseas, but I will take issue with your point. Maybe I'm agreeing with Bob, I'm not certain, but I think the problem of enforcement is a very real one. I think it's a real problem on both sides of the Atlantic. Now we've just been talking about Facebook, for example, now my organization EPIC, actually in conjunction with other consumer and civil liberties groups, brought two very successful complaints to the Federal Trade Commission about Google Buzz[31] – you had signed up for an e-mail service called "Gmail" and they decided you also wanted their social network service "Buzz" making your address widely available to all sorts of people. We objected to that. We said that was unfair and deceptive and similar things happened when Facebook changed its privacy settings. We said "unfair and deceptive." Lots of work, lots of good efforts at the FTC, and they announced great comprehensive privacy settlements. But then almost immediately it became apparent that the FTC would not enforce these settlements. The FTC would not enforce the settlements when for example Google consolidated its privacy policy across 60 services last year,[32] and it would not enforce the settlements against Facebook when it put out "timelines" resurrecting all your old posts, particularly the ones you really regretted, and now making them readily accessible. We sued the FTC to get them to enforce those consent orders. We thought they were good consent orders and we're not arguing about that. The judge basically said, "well, you have a very good point, seems like a real problem, I just don't have the authority to tell an independent agency to

29. For more information on FTC enforcement of privacy policies, *see Enforcing Privacy Promises*, FED. TRADE COMM'N, http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.

30. WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012).

31. *See In re Google Buzz*, EPIC, http://epic.org/privacy/ftc/googlebuzz/.

32. Mark Hachman, *Google Overhauls, Consolidates Privacy Policies*, PC MAG. (Jan. 24, 2012), http://www.pcmag.com/article2/0,2817,2399308,00.asp.

enforce its orders."[33] So that is where thing were left. But what's the point here? Enforcement has always been key. Bob is right about that. Enforcement is key but I don't think it's the situation where the EU just talks a good game. I think they actually do bring some judgments and I think we have a problem still in the U.S.

RO: I would just like to point out that you articulated fairly well where I'm coming from, but there isn't as much of a dichotomy. What I believe is I'm thankful that there are so many smart, intent people, lawyers, and technologists who are parsing these things and going at it. I just don't think it's anywhere near sufficient because fundamentally in my research in all this, there may be two or three out of a hundred people that really grasp what the data revolution is about and the enormity of it and the implications over the next 30 or 40 years. I don't think that all the good work that it being done in the legal debates, policy debates, is going to get the right kind of traction if you don't have that welling that is both emotional and determined by the middle class America – saying enough of the smoke making my kids sick, enough of the rivers that are burning like happened with the environmental movement. Until you have that, all this work is going to seem a little academic because the problem is only getting bigger and bigger and bigger by the day. So it's not as oppositional as you articulated.

SIV: Mary Ellen?

MEC: Taking that theme, Bob has talked a lot about the comparisons and non-comparisons to the environmental movement, Ryan Calo, who is now at the University of Washington, has this great metaphor along those same lines: around the same time when people were starting to get energized in the middle class, one of the things was about hunting of whales. In the 60s and 70s, across America, folks said who cares, who cares? And then there were some researchers who actually taped the whales singing, and you could hear the whales singing a song – it was actually popular, and played on radio stations, and it had a fundamental element that people could connect to. Then, all of a sudden, people started to say "you can't kill the whales," because they heard a human element or quasi-human element in there. And so I think part of the challenge for privacy advocates is, what is our whale song? We're getting drowned in data, the data revolution is taking place, but how do we articulate it such that you energize the middle class America? That's I think the question at hand.

SIV: So *Star Trek IV* was really a parable for the privacy information age?

Question: I actually had a related question to Mary Ellen's remarks just now. I think part of the barriers in the law that we are facing stem from this notion that once you've shared your information with someone, maybe your ISP or

33. *See* Elec. Info. Privacy Cent. v. Fed. Trade Comm'n, 844 F. Supp. 2d 98, 106 (D.D.C. 2012) (holding that "the FTC's decision whether to enforce the Consent Order is committed to agency discretion and is not subject to judicial review").

your cell phone carrier or someone else, that all bets are off for Fourth Amendment purposes. And the notion often comes up frankly with legislative battles, because what you share, well, law enforcement should be able to get it from those other sources and shouldn't have to get a warrant. And I'm wondering if any of you have thoughts on the best way to overcome that, whether it still is the courts because we at least had in Justice Sotomayor's concurrence in *Jones* a hint that the Court needs to reconsider the third-party doctrine?[34] And whether there is an avenue there or it just needs to be advocacy and done that through legislation of how we might overcome that notion that sharing with one person means that all bets are off on privacy?

MR: One of the themes of my class is that there is always a dialogue between the courts and the Congress about the scope of the right to privacy. And just because the Supreme Court says for example there is not a reasonable expectation of privacy as it did with telephone numbers in *Smith* v. *Maryland*[35] doesn't mean that Congress can't come along later and say in the Electronic Communications Privacy Act, "yes, there is," and maybe it's not the same as the content of the communication but we can still establish procedures if the government wants access to the telephone numbers that a person dials.[36] And you see this throughout the history of the right to privacy. I mean literally the tort of privacy was adopted by the Georgia Supreme Court but rejected by the New York Court of Appeals,[37] though the New York Assembly the next year by statute created a right to privacy that is with us 100 years later.[38] So I think your question is a good one, Sharon, but I think the trap here is to assume that because a court says in a particular context that it doesn't recognize a constitutional right to privacy, that that somehow ends the discussion. It has almost never ended the discussion in terms of the development of privacy law. There have always been other places to look including, by the way, state courts. You have lots and lots of cases. This is what *Maryland* v. *King* is about. The Maryland Court of Appeals said "no, you may not collect a DNA sample without a warrant," and so the Maryland Attorney General comes to the U.S. Supreme Court and says "well, I think my state supreme court has misinterpreted the federal Fourth Amendment."[39] We'll see what the outcome is, but I think the answer to your point, which a lot of people certainly make in the privacy community, is to never assume that there is an end point in the discussion about the right to privacy. If you don't like the answer at the first legal body go to a different one.

---

34. *See* United States v Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.).

35. 442 U.S. 735 (1979).

36. 18 U.S.C. § 3121 ("General prohibition on pen register and trap and trace device use").

37. Roberson v. Rochester Folding Box Co., 64 N.E. 442 (N.Y. 1902).

38. N.Y. Civ. Rights Law § 50 (McKinney).

39. 133 S.Ct. at 1965-1966.

EC: Or if you don't like the answer at the first legislative body go to a different one, because you have a lot of stuff being driven out of California. If you are talking about private sector actors and they want to act in California, they are going to be subject to California laws. So in data breach, and in a lot of these areas, you might have 49 different data breach laws. But if a company is acting in – and subject to the jurisdiction of any one of – those 49 states, they really have to act the highest standards so don't necessarily go to Congress but go to California.

GN: I think it would be interesting too to consider when you expose either data openly or third party data, distinguishing between what you know you are sharing and what you might not be aware you are sharing. I touched on this earlier, with regard to the *Kyllo* decision – flawed as it may be. If I expect that I've exposed certain data to my telephone company – who I call – it's possible to analyze a person's social graph the connections between who they call who they connect with and make determinations with no personal information or telephone information about sexual orientation, marital status, all that stuff, I may not have realized I was going to expose that, so maybe that should be protected or that type of analysis it should require more process or some kind of information to do that. I don't think there is a permanent solution and I think as soon as everybody gets home data mining kits, under *Kyllo*, it really wouldn't apply anymore. But it might be a stop-gap solution – are we conscious of what we are sharing, and if not, should the law be more protective of things that we are not conscious that we are sharing?

SIV: We're going to take one more question from Paul Rosenzweig, and then Bill is going to send us home. Paul?

Question: I'll make it brief. My question was very much made concrete by the very last set of comments, which was a suggestion that there should be jurisdictional informed shopping – and you suggested explicitly that that would raise the bar. My suggestion to the panel that I would like to comment on is that you've actually got it exactly wrong, that privacy wars will eventually trend towards the *least* common denominator as people drive off shore. The more important part of that is that cyberspace is globalized, and basically borderless and international in nature. Even if great privacy laws in the U.S. and EU eventually come together, what happens in China, what happens in India, what happens in Africa matters greatly to those people. American data gets off-shored there and outside of our jurisdictional control. So it struck me that you were reposing too much confidence in America's systems when maybe – I can't believe I'm saying this because I'm a Republican – we need an international answer.

SIV: I suspect that the panel will leave that opus out there, so please join me in thanking our panel for this lively and entertaining conversation.

APPENDIX I

Case Study CCTV with Facial Recognition and Terahertz Detection

A facial recognition system is used to link a photographic image containing one or more facial features to a database such that the actual identity of the individual may be determined. Facial recognition systems may use a variety of biometric identifiers, including face topology. New techniques incorporate 3-D modeling, which may improve accuracy. Facial recognition systems typically require a database of identified images and techniques that enable the sorting and matching of many images in a few seconds.

Terahertz technology makes possible the identification of chemical composition at a distance. In some applications, Terahertz may be used to detect the presence of contraband, such as explosives, narcotics, and concealed weapons.

The Department of Homeland Security is considering the deployment of Second Generation Municipal Security Networks ("SGMSN") system that incorporate CCTV, facial recognition, and terahertz screening.

At present, the Department of Homeland Security provides grants to local and state government for domestic security. These projects include the deployment of CCTV systems that enable the real-time surveillance of public areas. At present, the DHS has not determined whether to provide funding for systems that include facial recognition technology.

- What Fourth Amendment issues arise from the deployment of the SGMSN system?
- What Privacy Act issues arise from the deployment of the SGMSN system?
- May the government mandate the installation of these SGMSN systems on private property?
- Should the data be merged with other record systems?
- Should the system be used for policing functions?
- Should the system "alert" to behavior that is objectively suspicious, *e.g.* breaking a car window?
- Should the system "alert" to factors that are objectively suspicious, *e.g.* an outstanding warrant?
- If alerts are integrated, should the algorithm be made public?
- Should records of alerts be maintained?
- Should the system be deployed during political events in Washington, DC?

After you have answered these questions and developed best practices, the Secretary has asked you to consider one further question:

- Should the DHS provide funding for these systems?

APPENDIX II

Case Study Multinational Advanced Travel Data Exchange (ATEX)

Passenger Name Records (PNR) are created by air carriers to record and manage travel reservations. Air carriers also collect data from the biographic page of a travel document, known as Advanced Passenger Information (API), at check-in. Border security authorities in the United States and abroad collect PNR and API data from air carriers, combine it with other government data sets and use the resulting risk assessment to prioritize border inspection resources on travelers perceived to be of a higher risk. The use of PNR has been controversial for privacy reasons – e.g., the transfer of bulk commercial airline data on mostly innocent purposes to government databases for risk assessment purposes, as well as concerns over the accuracy of the underlying data. That said, the Department of Homeland Security (DHS) maintains PNR-based risk assessment is an effective tool against terrorism and organized crime – to wit, all international travelers are already subject to inspection anyway, and automated risk assessment enables resources to be focused on higher-risk travel. Other jurisdictions have followed suit: the European Union has finalized a PNR Directive of its own (subject to ratification by the European Parliament), and numerous other countries are establishing PNR and API-based risk assessment systems.

National authorities to collect API and PNR are, however, generally limited to travel that touches the nation in question. The dynamic nature of international travel means that malicious actors often travel through multiple countries – with stops along the way – before departing for the target destination. Hence a complete picture of an individual's travel is possible only through pooling PNR itineraries together across national jurisdictions.

Accordingly, in this fictional case study, DHS, DOJ and several like-minded interior ministries abroad are considering a proposal that a multinational Advanced Travel Data Information Exchange (ATEX) be established to share PNR and API information, consistent with each data contributor's privacy policies. Such an approach is also said to offer cost advantages for both air carriers and participating nations by enabling centralized connectivity between air carriers and participating governments through a central pipe, rather than multiple repeat connections, as well by standardizing the parsing and formatting of the data.

- PNR and API data would be collected in a centralized multinational data warehouse, subject to appropriate IT security protections. Data sets would technically be owned by the country with authority to collect that data.
- The data warehouse would offer centralized identity resolution capabilities – i.e., the ability to correlate multiple PNR records to a single trip, as well as to correlate API and PNR records for the same traveler.

- Data related to international travel for a participating country would be pushed to that country for comparison against national watchlists and rule sets, as well as pre-departure authorization if the appropriate service levels can be established.
- Participating countries could also permit third countries certain levels of access to their data, e.g. –
  - Full access
  - Access to non-PII data.
  - A more limited ability to run federated queries – either historical or persistent – against its data. Hits could either be forwarded automatically or require manual approval before they are shared.
- Third country access would be country and role-specific – to wit, differing levels of access could be enabled for different countries and different authorities within those countries.
- Participating countries can also participate on a "query only" basis – e.g., not contributing data, but submitting queries against data in the repository. Query responses would be handled according to the data owner's privacy and information sharing policy.
- A collaboration space would be established where countries can share anonymized demographic and routing data related to known travel-related seizures and arrests for the purpose of building knowledge-engineered pattern-based risk rules.

Questions for discussion:

- What Privacy Act issues arise from the deployment of ATEX, to the extent the U.S. Government were to participate?
- What key privacy protections might be drafted into the charter of the data exchange?
- To what extent does a federated architecture add privacy-related complexities to redress?
- How can technology and system design be leveraged to mitigate privacy-related risks?
- What are the privacy-related implications of choices concerning where the data exchange might be housed?
- How does the analysis change if data ownership falls to the data exchange rather than participating countries?

***