The John Marshall Journal of Information Technology & Privacy Law

Volume 29
Issue 3 *Journal of Computer & Information Law - Spring/Summer 2012*

Article 4

Summer 2012

Session III: Privacy Regulation and Policy Perspectives, 29 J. Marshall J. Computer & Info. L. 343 (2012)

Leslie Ann Reis

Mary Ellen Callahan

Renard Francois

Peter P. Swire

C. William O'Neill

SESSION III: PRIVACY REGULATION AND POLICY PERSPECTIVES

Moderator:

Leslie Ann Reis
Assistant Professor;
Director, Center for Information Technology and Privacy Law, The John Marshall Law School

Panelists:

Mary Ellen Callahan
Jenner & Block

Renard Francois
Corporate Counsel, Caterpillar Financial Services Corp.

Peter P. Swire

C. William O'Neill
Professor in Law and Judicial Administration, The Ohio State University Moritz College of Law

PROFESSOR SORKIN: Our first session this morning will examine privacy regulation and policy perspectives. The moderator will be my colleague, Professor Leslie Reis, Director of the Center for Information Technology and Privacy Law at The John Marshall Law School. Professor Reis.

(Applause.)

PROFESSOR REIS: Thank you, Professor Sorkin. And thank you all for being here at 8:40 on a Friday morning early. We appreciate that very much. We have three distinguished speakers this morning: Mary Ellen Callahan, Renard Francois and Professor Peter Swire, all of whom have extremely impressive resumes containing both public and private sector experience. Each will have twenty to twenty-five minutes, give or take, to present their various perspectives on privacy policy and regulation. I want to leave significant time for questions and discussions.

The name of the symposium is: The Development of Privacy from Brandeis to Today. And each panel so far has made mention of the famous Warren and Brandeis article, "The Right to Privacy," written in 1890—122 years ago. It's the starting point for our exploration of privacy this morning.

And before our speakers begin, I want to give just a little background and context for at least some of the driving forces underlying privacy policy and regulation in the U.S. And instead of getting all professorial on you at 8:40 on a Friday morning and ramble on about the developments of privacy during the past 122 years, I present to you instead a chronology of privacy drivers in a minute and twenty-two seconds.

(Whereupon a video was shown.)

PROFESSOR REIS: And given my exuberant application of the fair use doctrine, I am keeping Professor Doris Long on retainer. Thank you.

Our first speaker is Mary Ellen Callahan. She is a nationally recognized privacy attorney with an extensive background in consumer protection law. She is currently, and very recently, a partner at Jenner & Block, having just left her post as the longest serving chief privacy officer of the U.S. Department of Homeland Security. Ms. Callahan will present her perspectives on privacy policy development in the public sector.

MS. CALLAHAN: Good morning. As Professor Reis said, I'm Mary Ellen Callahan. I am now a partner at Jenner & Block, but I'm going to probably primarily talk about the Department of Homeland Security and how it has attempted to integrate, or embed, privacy protections in the

privacy policy development, as we said. Just a little bit of perspective. I'm not going to stick closely with these PowerPoints, but I thought it would be good for framing our conversation about privacy and ways to think about privacy, specifically in my case, privacy policy development in the public sector.

Many of you, but maybe not all of you, know that the Department of Homeland Security's chief privacy officer was created when the department itself was created, so that's 2002, the first privacy officer being in place in early 2003. The privacy office reports directly to the Secretary. It's a department-wide position. What does that mean? Those of you who are in government know that there's a lot of policy issues, a lot of broad issues, and a lot of kind of headquarters-is-getting-in-our-business type of scenario.

There are seven operating components, many acronyms that you guys are very, very familiar with, and I'm happy to talk about it in the question period—TSA, FEMA, ICE, U.S. Citizenship and Immigration Services, U.S. Secret Service, Customs and Border Protection. So those are kind of what we call the operating components.

And that's where Homeland Security interacts with people every day and at a number and a scale that's almost hard to believe. Customs and Border Protection processes about 650,000 people crossing the border every day. TSA processes an additional 1.2 million people flying every day. Citizenship and Immigration Services will process people through the immigration service and have naturalized citizens in a couple million every year. So the scale itself is quite extraordinary. And they deal with privacy all the time. And they deal with circumstances all the time. And again, I'm talking about privacy policy development.

But at the same time, one of the things that I try to explain to my colleagues is the least common denominator. Your interaction with TSA is going to color your interaction with the Department of Homeland Security. We're not always successful on that, but we're trying. But to understand that each individual—the whole point of privacy, it's an individual right. And so individually you have to think about that.

The Department of Homeland Security, in addition to those operating components that deal with privacy with individuals so frequently, we have three department-level directorates or offices with specialized experience, which I have listed here: Intelligence and analysis, which actually have slightly different privacy rules but ironically ended up being one of my biggest allies at Homeland Security, and we can talk about why later on; science and technology, so all the research, all the super scary stuff that you see in Tom Cruise movies primarily, or science and technology is working on, and the number of hits that they have is probably a pretty low percentage, but we want to make sure that they're think-

ing about the privacy stuff and that we're integrated in the very earliest process; and kind of a hodgepodge directorate called the national protection and programs directorate, which has among its many qualifications cyber security, infrastructure protection, which is liaising with the eighteen different sectors of critical infrastructure; and then the federal protective service, which are the people who protect the federal buildings. And so that's kind of an overview of the department and how it sits.

A little bit about how the department and I constructed the way to implement privacy policy development in Homeland Security specifically. And Homeland Security, I've got some of the numbers here; we have forty-five people, in what used to be my office, divided up into these areas of policy, advocacy, compliance and transparency, and oversight.

And watching Leslie's video and how it intersects, all of those issues were addressed, even in a fair use way, in her video and that's why it's important and that's why we reorganized the office to break it down into these different areas. Almost everything we do has a policy element. But is it compliance with policy; is it compliance with the Privacy Act of 1974 or FISMA of 2002, which are my two big statutes? And I'm going to say "my," even though it's not mine anymore, so you'll get the idea.

So we've broken it down into these elements. I mentioned the seven operating components and then those three department-wide policy components. And so by the instruction of the Deputy Secretary, each of those privacy officers—there are ten component privacy officers who have much more of an implementation, not a policy bent, I do kind of the broad-brush policy for the department – but they go and look at that and then they go and implement it. They also go and look to see what new technologies are happening. They're getting involved in what's happening within their department. And they have reporting directly to the component front office, which is to make sure you have visibility in what your whole component is doing rather than being siloed in one area.

DHS has 125 privacy professionals, titled privacy professionals, overall, which is by far the largest privacy practice in the federal government. And I would say rightfully so, right, given the scope of the issues that I talked about.

So what do we do? Right, 125 people. What are we working on? And how are we working on privacy policy development in the public sector? As I mentioned, my authority is to implement the Privacy Act of 1974, which is to do system of records notices, to do notifications of the same. What do we do with information? How are we doing it? And to do that ahead of time, ex ante as we say in law school, and to make sure that that is available so you say: What's your authority to collect the information? With whom are you sharing it? How long are you storing it? And how can I get access to it?

Right. So applying the fair information practice principles in system of records notices. In addition, we do privacy impact assessments that are required under FISMA, again ex ante, and again to try to go and give a transparency document to explain what's going on with the document.

One of the things that we've done with the privacy impact assessments, that I don't know is clearly described, is the privacy impact assessment is both a document, the end document that's published on the website that's talked about, but it's also a process, right, so we have a framework, we have a checklist, where you would go through the process. And if somebody says "I would like to capture everybody's DNA when they come to the border"—which, by the way, is not a plan, I want to be very clear—using a hyperbolic plan—but so if you go and say "I want to capture DNA at the border for every person crossing in," then we would go and say, "Okay, what's your authority to collect that?" "Okay, that's probably a little shaky." "Okay, so what are you trying to do?" And you would work with the program managers, the component privacy officers would work with their people, and then we would also come in and say, "Okay, what are you trying to do? What's the goal here?" "Oh, the goal is to make sure we've got proper identification for people coming in, we don't have people crossing the border multiple times in the southwest border." "Okay, maybe you can do that with collecting less information. Like let's try to figure out what you're collecting, what you're doing and how you're doing that."

And it's a balancing act. And so that whole process and that give-and-take and that back-and-forth is not memorialized in the final privacy impact assessment. What are memorialized in the final privacy impact assessment are the rules of the road. What the Customs and Border Protection can do with their collection of, let's say, fingerprints. And what they can do with them and what they can't do with them and that's what the transparency document is. But the whole discussion of DNA is not in the document; it's not in the process.

And so some people have said, "Well, that means you're not doing your job because you just rubber stamp what they're doing." Trust me, I do not rubber stamp. And my office does not rubber stamp. It's a dialogue. It really is a privacy policy development as is the title of my program.

But in order to do any privacy job, you have to have allies. You have to have people with whom you can work. Because if the privacy office is standing to the side saying "No," then people are going to be like, "Okay, we're just going to go around her," right? We're going to go and say, "All right, we'll find another way around that."

And so I've listed several of the allies that Homeland Security privacy had. The Chief Information Officer is a pretty self-evident one in

light of the technology issues, the transition to cloud computing and all sorts of issues, particularly in this administration, but just in general, and I think it will continue to increase in the future in terms of technology. And can we find privacy-enhancing technologies, that's a whole subset of conversations that we're having with the CIOs and the federal privacy officers overall.

Officer for Civil Rights and Civil Liberties. I put that there. It is not a typical privacy officer liaison, right, but Homeland Security has an office for civil rights and civil liberties and I'm statutorily required to work with them. I put it there because, number one, they're a great ally. And it's really useful to have people come at it from two different angles but have the same conclusion, but also that the privacy civil rights and civil liberties issues, as you guys are learning in this session, are so intertwined. Office of Policy, which is a department-wide policy.

Office of Intelligence and Analysis. As I mentioned to you, they were a fairly good ally for me because they needed to get stuff done. They needed to do information sharing. Well, information sharing has a lot of personally identifiable information. There is a requirement that the Department of Homeland Security share certain types of information. And they couldn't figure out how to do it. And so we actually came in, and they said, "Well, you know, let's just drive the database over and just give it to them." And "them" could be the Federal Bureau of Investigation; it could be the National Counterterrorism Center. I'm happy to talk about both of them in Q&A, just an FYI. So it could be that.

And you're going to say, "Okay, well, let's figure out what you need to give them and what you don't need to give them." And we actually designed a program that's pretty privacy protective and is a good model for the rest of the federal government but also meets the statutory requirements to share information.

General Counsel is an obvious one. Although I will admit I was not a lawyer in my job at Homeland Security. It is a policy position, not a legal position, as I was reminded every day by the Office of General Counsel. "You can't analyze that." "Yes, I can, I swear." Office of Inspector General, from the oversight perspective, the components that I talked about already.

And then the other department privacy officers, which are, there are privacy officers throughout the federal government. They're in very different areas, very different stages, and very different parts of their department or agency. Some are in the CIO's office. Some are in the Office of General Counsel. Some of them are in policy. I mean, they're all scattered all over, and I think that affects their utility.

But what we have done is create a privacy committee so that you can share best practices. Because a lot of the stuff we do does not need to be

repeated, does not need to be reinventing the wheel, but to try – for example, we had several pieces on social media and what's the federal government's use of social media. And in the materials for the conference I have my testimony on DHS's use of social media. I testified in front of the House Committee on Homeland Security in February on that.

And the issues are very interesting, because I used to represent a very big social media company before I went to DHS. I was like, I know all about it, I know the technology, I know the way it works, and I know the processes. And then you layer on top of that the First Amendment and the Privacy Act and, you know, conspiracy theories of government spying on you. And you get all this stuff and it gets really complicated and it gets really thorny.

And what we tried to do at Homeland Security from a policymaking process is there are basically three ways that the department uses social media. The first one and the one that took a long time to do, which is kind of surprising, but if you think about it it was a good start, is the pushing out of information. The Twitter accounts from DHS or from FEMA. FEMA has got a phenomenal social media program and that's great and that's really important. So the pushing out of information, the communication of information, in terms of, you know, kind of broadcast but in different vehicles. And what are the rules of the road for that? So we have a privacy impact assessment for that. And say if you adhere to these standards in the privacy impact assessment: Don't collect PII, don't communicate with people, make sure it's clear that you're the Department of Homeland Security, don't use non-DHS computers, and so on, then you can go ahead and we'll just keep track of it. We have an attachment in the privacy impact assessment that says: These are all of the officially sanctioned accounts.

And if you don't want to meet those standards, okay, fine, but let's go through the PIA process, shall we? You know, let's go through: Why do you need this? Why are you doing this? Why are the standards that the department did overall not sufficient for you, FEMA, on the social media campaign?

And some of them have done that. But mostly people are like, yeah, you're right, the DHS standards are good. That's right, the DHS standards are good. And that says that you get the broad framework and then you go and see, do we need changes, are the missions different?

Then the next set of areas where Homeland Security uses social media is in a situational awareness circumstance. And the situational awareness circumstances are very—it's interesting, because a lot of other departments are like, ah, everybody can use social media and everyone can follow on Twitter. And actually, at Homeland Security, it's a

lot narrower because what we decided to do is there's the ick factor of you feel like you're being followed by DHS.

So there is an Office of Operations that has a requirement to keep the President and the Cabinet aware of natural and man-made disasters, so basically, emergencies, terrorist attacks, and other natural disasters. And so we have a scenario, we have a very small group of people who can do certain elements with social media that they can follow on Twitter, and they have the series of other kind of white-listed places that they can go. They can't collect PII unless it's in very narrow circumstances, like a federal official speaking in his professional capacity and those types of circumstances. And we actually audit it every six months. We go and look at it to see: Have you collected too much PII? What's in the storage? What are you doing? How is this going out?

And it's been very successful and I think it's a very good kind of balance of keeping people up to date. Because we all remember Katrina, that, you knew and you knew and you knew and I knew, everyone was at the Super Bowl. Well, Michael Chertoff didn't know everybody was at the Super Bowl, because he didn't know that, because he didn't have it verified by two federal officials. That used to be the standard of when you would tell a Secretary or somebody at that level.

Well, now, that really didn't work out very well. And so that's it. The idea is, okay, if we know, then really the people who can take action, FEMA, for example, should know. And so we went through this whole process and I think it was a very successful process.

The third area that we have is the use of social media for investigatory purposes. And there are very different responsibilities and standards, candidly. U.S. Secret Service has a different mission set and has a different set of standards than U.S. Citizenship and Immigration Services do.

But what we did in the privacy policy development of the department is we wrote a management directive, because we love directives in the government, we love process in the government, and actually I'll go to that slide. So the management directive was written on social media for investigatory purposes. And then it says you have to have these eight standards, which include clearly identify yourself as DHS, use DHS computers, don't friend people, you know, having all of these different types of standards, eight different categories.

And then it says, if you have reason to be undercover, tell us about it. I'm Secret Service; I have reason to try to check to make sure that somebody is not having a threat to the government. These are my standards by which I do that, right? And they would actually tell us, when you say, okay, you don't have to adhere to the seventh of the eight categories or things like that.

And so again, we have broad standards so the whole department will apply to it. And then you can go and explain why am I different, right, and why is this different, and to document it, and then we go back and we are scheduled to check it. I won't be there, but we're scheduled to check it.

And that brings me to kind of the final point, which is, you know, we're talking about privacy policy development, but I also want to talk about accountability, which is one of the fair information practice principles, and it's an important tenet for privacy overall and for privacy in the public sector in particular. Because transparency and accountability are really important tenets of our government and of our democracy.

And so even though we've got all these privacy officers upfront, even though we have all of these people working in the front end and we've got all these great directives and that sort of thing, well, you want to make sure: Is it just paperwork, or are people actually applying it?

And so we have instituted a series of different types of privacy oversight to kind of close the loop and to make sure that the whole life cycle is being implemented.

There are three different types, kind of the most extreme to the least extreme, and there's obviously policy and advocacy in between. But the first one is an investigation. And my office is fortunate and unique to have the ability to investigate anything in the Department of Homeland Security. There is no restriction. And I actually think it's implicit that it involves personally identifiable information but not exclusively.

So what does that mean? What did I decide to use that investigatory authority for? I've used it three times when I was there, and the first three times that the chief privacy officer has ever used it, and they all involved significant noncompliance. It wasn't an oops. One was a breach, but it was a very egregious breach. It involved significant noncompliance and they involved circumstances where you could use this to be a learning tool to be a best practice for the rest of the department.

So the areas where we had it, first, we had it with the Inspector General. I investigated the Inspector General, which was actually kind of cool. But it was pretty collaborative, they actually did the fact-finding and then I did the privacy analysis. Because I think that's fair. They're much better at fact-finding, that's their job.

And they had an unencrypted USB drive that their financial auditors used and that they passed down from generation to generation, because it was too hard to log into the DHS system, pull it off, and then do the analysis they needed to do for financial systems.

The Inspector General's office had no idea this was going on. But the auditors, again, would pass it down each year like some gift to the next auditors. And they lost it. And they didn't know what was on it.

They didn't document it. And it had Immigration and Customs Enforcement personnel information; it had U.S. Citizenship and Immigration Services, Customs and Border Protection information, all this information, unencrypted, violating DHS policy. Sharing the drive violates DHS policy. Uncataloged violates the DHS policy. Keeping it on there for more than ninety days violates the DHS policy.

And so what we did is the Inspector General and I worked together to go and say, okay, all of those are bad ideas. And technically, the contractor, according to the contract, didn't have to adhere to DHS standards. Well, we needed to ameliorate that, didn't we? So that was one example of what we did. The second example of what we did was actually social media. What we did with social media, and that a component was inappropriately using social media, we did not yet have that management directive I talked about, but that was the basis of it, that I went and created it.

And the third area was interesting, where somebody was sharing information because they had to, and they had to, and it was a national law enforcement national security issue. Didn't encrypt it. Didn't have an agreement. Didn't have processes. Never had a feedback loop for the law enforcement agency they shared it with to find out: If they had a bad guy, did they ever tell us? No. So does that mean there's no bad guys or you just didn't tell us and we have the bad guys still in our office?

And then that, too, also had ramifications. And I think that's really important because it's important to be able to say: If you guys really mess up, we can come in. There can be different investigations.

I worked, while I was there, there were eleven Inspector General investigations and six GAO investigations involving privacy at Homeland Security. So we definitely are getting other investigations, it's not just relying on me and my little staff. But I think that that's useful to know. Because you have different angles, you have inside, you have outside, and so on.

A privacy compliance review, that's what I did with social media and the situational awareness. And is, you go in, you look, are you still adhering to the standards, are you still working on that? We've done it for several other things including suspicious activity reports and other elements. And those are all available on our website, and I think that's very useful.

And then just generally dealing with compliance and integration for data breaches or other types of things where we've had more experience and we can help the components as they each do it.

All of those are to say that privacy policy development in the public sector takes various forms and this is the way Homeland Security does it, but I think it's a useful way and a useful framework to think about

how to do privacy policy development in the public and maybe even private sector.

Thank you.

(Applause.)

PROFESSOR REIS: And thank you very much. Our next speaker, Renard Francois. And among Renard's many resume items is he is a graduate of our LLM program, so we'll start with that. Mr. Francois is currently the corporate counsel in Caterpillar's Financial Treasury, Securities and Compliance Group where he focuses on anticorruption, expert controls, anti-money laundering, privacy data and security, and Fair Credit and Reporting Act.

Prior to Caterpillar, Mr. Francois did serve as an attorney at the private firm of Bass, Berry & Sims in Nashville. And prior to that he worked for the U.S. Federal Trade Commission in Washington as an advisor to the Consumer Protection Director where he focused on privacy, identity theft, and the Fair Credit and Reporting Act. He also served in other capacities with the FTC, and his talk this morning is the Industry Perspectives on Privacy Regulation. Mr. Francois.

(Applause.)

MR. FRANCOIS: I do not have a PowerPoint presentation, so Mary Ellen showed me up a little bit. And it has been a pleasure to come back to John Marshall and see all the great things that you're doing at the school, see the great developments that are going on, and you've got a very bright future here with the school with the Center for Information Technology. So it's been wonderful. So I thank Professor Sorkin and Professor Reis for the opportunity.

I've had a chance to work with Mary Ellen on the Data Privacy and Integrity Committee, so I've been fortunate enough that she kept me on before she abandoned me, and so we've had a chance to work together.

What I wanted to do was talk to you a little bit about my experience in each of the areas of where I've worked, from the Federal Trade Commission all the way through to private industry. Because the privacy issues that we confronted and the privacy issues that challenged us changed. And just like the privacy issues from last year are going to be a little bit different from the ones this year and they're going to be different from the ones twenty-four months from now, I think we can get a good sense of kind of what that change was, what people were concerned about, and what some of the challenges that we faced were.

My quick plug is, you know, it's funny, because a friend of mine told me about the LLM program here, and so I came from Washington, DC,

out to Chicago, knowing only a couple of people, to do the LLM program, and then partway through got a job opportunity at the Federal Trade Commission. So where I am now and where I have been professionally wouldn't have happened without the experience and the exposure that I got here. So they've done a wonderful job programmatically, and I just wanted to tell both Professor Reis and Professor Sorkin thank you, because it provided tremendous opportunity.

So when I was at the FTC, the FTC's main charge is to prohibit, or to stop, unfair and deceptive acts and practices against consumers. So the FTC is the country's consumer protection agency. And when I started, the reason I got the job out there as a staff attorney is because we had just initiated, the FTC had just initiated its Internet fraud program. And this was back in 2001 where the challenges in the Internet fraud were people were getting these e-mails or going to websites that were taking advantage of them, taking them into different websites and multiple-click sites and, really, they called it page jacking at the time.

And so one of the things that we wanted to do at the Federal Trade Commission was investigate Internet fraud as well as teach local and international law enforcement how to investigate Internet fraud and bring those challenges.

So really, our big focus there was spam, unsolicited commercial e-mail. Websites that looked very similar but weren't what you were looking for and would take you to different places or take you to places and advertise that you'd win something and when you'd call to get your prize and you ended up paying for a 1-900 number is one of the largest cases I brought.

And so the challenges then, and particularly for our Consumer Protection Division, were two. So we had the Internet fraud side, but we also had kind of the representations and warranty side. What are institutions saying, particularly customer-facing institutions, about their privacy policies? How are they going to handle your information?

Because at that point in time, privacy policies were somewhat new. But how to use them and how they can be used or how they could be used against a company was pretty new. I mean, they had websites that told you what the terms of service were but didn't really clearly tell you what they were going to do with your information. People were trying to monetize the information that they had in the Internet and finding new ways to create revenue over a fairly free system. So those were two of the big challenges that we had is, one, how do we educate consumers so that they don't get duped online, and then how do we take action against those who are trying to dupe consumers.

And then the other side of it was for the legitimate companies, what are they saying about the information that consumers are giving? What

do they need to say? And we had a number of—I started when we had just started establishing the foundation of data breach cases. And I remember by the time I got to the attorney advisor's office, we were now starting to really formulate a policy that related to, one, not every data breach is a violation of the FTC Act, that a violation of the FTC Act can occur if there is a breach that's attributable to a widely known vulnerability that a company doesn't take action against.

One of the other precedents that was established in one of the cases is that companies don't have to eliminate all data breaches, just those that are—they don't have to have perfect security, they just have to have reasonable and appropriate security in light of the information they have.

And so really, it was an effort to try and not be so prescriptive in terms of what a company should or shouldn't do, but more so, how should a company look at its own system, assess its own risk, and then take reasonable steps to mitigate those risks of data breach. I was actually there when we sued Tower Records, who was trying to do the right thing in terms of increasing their security, but someone forgot to include the authentication code in the website and that allowed for a period of time anybody on the Internet to go to the Tower Records website and input five random numbers and you'd see the associated customer record that was associated with those five numbers. It was a mistake. They were trying to be good corporate citizens, but they made a mistake and it still got them sued and established the precedent of intent is irrelevant.

And so we were there in those very beginning times where we were trying to figure out how do we use the privacy safeguards rule? How do we get companies to be more proactive about privacy of their customers and their consumers? What are they going to say in their privacy websites and, after they say it, are they adhering to what they say?

So we essentially view privacy policies as an aspect of marketing. It's a statement that—and is it a misstatement? And with respect to privacy, we considered it a material statement. So if you omitted it, it was a material omission. But if you said something, it was a representation that you were going to have to follow through with. And I would speak to different companies or industry groups or talk to other companies at the FTC that said, "Well, why don't we just not have one," or "why don't we just not have a provision in our privacy policy or terms of service that relate to privacy?" And the answer was simple at the FTC, we would just call that unfair, which is probably the worst classification you could have at the Federal Trade Commission. Because if you're deceptive, at least you can cure it with an accurate statement. If your business practice is deemed unfair to consumers, you just can't do the business practice.

So the FTC was really, I think, pushing the line and pushing the envelope in the privacy practices. And it was interesting at that time, when I had come there was a transition between chairmen, and so it was interesting to hear anecdotally that the previous chairman was reluctant to use the unfairness doctrine to attack businesses or to sue companies, but the current chairman was more than happy, for the appropriate case, to use the unfairness doctrine.

And I remember being in a meeting in his office and he said, "Well, if it walks like a duck and it quacks like a duck, it's unfairness. And why wouldn't we call it that?" And so it was very different to see them on the very cutting edge of trying to implement these policies and procedures in not just what we call the Section 5 cases, which are the unfair and deceptive cases, but also the policies and the rulemaking procedures and in safeguards rule. And when we were there, there was also the amendment to the Fair Credit and Reporting Act, the Fair and Accurate Credit Transactions Act, which had a very heavy emphasis on privacy and reducing the risk of identity theft through the different amendments to the Fair Credit and Reporting Act and the new rule provisions.

So it was an interesting time to be there and it was an interesting time to kind of see the impact on the industry, to be a fly on the wall in some of the meetings that industry and consumer advocacy groups had with the bureau director and also the chairman about how privacy policy could either complement or undermine private practice approaches or business approaches. And so taking that, I then moved to Nashville, Tennessee, which is my hometown, and went into private practice in intellectual property litigation and also general litigation as well. But the areas of privacy where I tended to focus my time and energy was on financial privacy, health privacy, and some data breach resolution. The interesting thing that I learned there is just a real pragmatic idea of there are certain drivers, what I'd call driver regions in terms of policy and privacy. And Nashville wasn't one of them.

And what I mean by that is when you're out in New York or Washington or Silicon Valley, there are people who understand how you can influence legislation in a way that by being part of the process, by being either part of the rulemaking process or submitting comments for a rule. Some people think that those comments go someplace and they largely get ignored. Many do. But sometimes you get them from very big companies or industry groups, where they're not just submitting comments online, they're also submitting comments and having meetings. And that's a way to really influence what a rule or a regulation looks like.

And I remember when we were going through the CAN-SPAM Act, because that happened while I was at the FTC, there was an Internet industry group, and there was a particular company that was the most vocal in that group. And they actually got a clause inserted into the law

that, you know, it was funny, they got a clause inserted into the law that caused the FTC to do about a year and a half worth of rulemaking, but then they also got something else that wasn't favorable to them inserted. But seeing that and seeing how they advocated for their industry and on behalf of their business practices, there's a direct correlation when you look at that clause that those efforts led to that. And ultimately, because it was rulemaking, there is a rule that was caused by those efforts.

So there are a lot of cities where you've got a lot of law firms and businesses that don't really—they're more receptive to the regulation as opposed to really trying to get to be part of the system to try and move it in a certain direction.

And so that was one lesson learned being in Nashville and trying to talk to clients as an associate, you know, sometimes you're dumb or fearless in life, and going to a partner and telling them that they should talk to a client about doing X, Y and Z is not usually how the system works. And there are a number of ways, a number of instances where I've done things like that. But you found that people were less receptive to that. So the focuses in that industry were financial health care, because it is the health care capital of the United States, essentially, and occasional breach work.

And now, as I'd left the FTC and through my time in Nashville and private practice, data breaches were becoming more pronounced. There was more focus from the Ponemon Institute about the cost of the data breach and its effect on customer satisfaction. And they'd just started doing research on its effect on customer retention.

And trying to get companies focused on that in the Nashville and middle Tennessee area was a really difficult thing to do, because it was more a brush fire. If we have a breach, we get somebody in to fix it. Tell us what we need to do to fix it. As opposed to, what do we need to have in the front end to really make sure that this doesn't happen?

And so that was a challenge and a challenge I saw that—and talked to colleagues—that outside, I think, of certain communities that was a challenge that a lot of people in the privacy community and the privacy practice community faced in certain markets.

And it makes sense, now that I'm on the business side of it. Because if you translate it to me as an in-house attorney, that means a private practice attorney is saying: "Let me charge you by the hour to understand your systems and then give a report that you will then implement and the bill will be like $25,000." That's not palatable. And so how do you incorporate those?

So it's a hard pitch to make at that time in 2003 to companies that hadn't really experienced or been burned by a data breach. And most of

those companies were not multinational companies. And that was another aspect of it too.

So then I went to Caterpillar and was somewhat interested in going. I love Nashville, I love my home, but I had an opportunity to go to Caterpillar. And I remember the conversation I had with my wife and also with the folks in Caterpillar, and it was, if you read the job description, it looked like they didn't know what they wanted. They didn't know what they wanted the privacy person to do at CAT, Inc. And I said, "Well, that's either a good thing or a bad thing." I mean, if they want me to focus on HR privacy issues, then I'm not really interested. But if they really don't know, if this is really as open-ended as this job description looks like and they don't know what they're doing, that's something I'm interested in, the ability to go in and kind of create something and figure out how do you build a program within a large multinational company.

And they didn't. I mean, they would readily say "We don't know, we don't know, here is what we think, but we just have no clue." And they had some incidents in the past that led to a Six Sigma team that led to the creation of this position that they were trying to fill. So off to Peoria, Illinois we went.

And the big challenge, I think—and just to take a step back, before I interviewed with Caterpillar, I knew they made machines. But if you told me they made pogo sticks, I would look at you and go, wow, that's interesting. So I had limited knowledge of what Caterpillar did and what their privacy issues would be. And when I talked to people when I was at CAT, Inc., they'd say, "Well, what are some of their privacy issues?"

Well, I'll give you an overview of what the company does. You all know they make big, heavy machines, the yellow equipment. But they also have, amidst their 300 to 400 subsidiaries that fall underneath CAT, Inc., they have CAT Financial, which is a wholly-owned financing company which operates and has at least branches in thirty-four countries throughout the world; they have Progress Rail, which is an international rail remanufacturing company which is located in Alabama; Solar Turbines, which is another multinational corporation which creates and sells turbines; Perkins Engines, which makes engines, I think they're based in Ireland, they might be a little bit older than CAT itself; they also have Bucyrus, which is a large international mining company. So if you have a mine, Caterpillar—it may not be branded as CAT—but the CAT, Inc., company can provide you ninety-five percent of everything you need, from the truck and the equipment, in the CAT, Inc.

So that is everything, almost everything that falls underneath—and then there's the logistics company. So they can ship parts and services

all over the world within a twenty-four hour period. So that's all that falls under the CAT, Inc., umbrella.

And within that we have clearly, you know, you've got clearly employee relations issues, employee issues with their data. But also we work through a dealer network and so these dealers aren't our agents, but they're licensed to sell CAT equipment, so they are the interface with the customer. We are the interface with them. Those are two more interfaces where we get personal information from all over the world.

And then, even within the CAT, Inc., you've got international business units, like global information and security, global human resources, and the global export controls compliance business unit. So it is a heavily matrixed worldwide organization that really had no concept of privacy and how to incorporate it into eighty years of business practice.

And so my job was, with a staff of me and a budget frozen in 2008, to come in and create and fix it. Those were my marching orders—just fix it. We're going to put you in an office—fix it. And you're going to report to somebody that has health and OSHA, that does OSHA and does import-export and privacy—just fix it.

So I'd go in every day and try and fix it. And it was like playing racquetball, because all of these business units are developing their own projects and their own—and many of them are good—trying to drive efficiency, trying to share information. But we had no concept of how do you operate in a worldwide organization.

We had a code of conduct, we had a policy on data privacy, we had websites, but no one integrated those into business practice or the business considerations. And there were a couple of things that I focused on in terms of investigations and how you collect certain data, but it was a drop in the bucket.

So what we ended up doing was making a recommendation—I'll never forget this – on December 17, because CAT, Inc.—the legacy of a manufacturing company is the shutdown between Christmas and New Year's, and so you're just trying to make it to shutdown, that's what you hear in December, everyone make it to shutdown.

And I'll never forget my meeting with four global vice presidents was on December 17, in the afternoon, 3 o'clock. They'd all just heard that they're getting budgets cut and I'm coming to them saying "Well, now, you've got to pony up some money to create this compliance organization, this data privacy and information security committee."

And the CFO just went crazy. And it was funny to see the other vice presidents just kind of sit back, like, well, let's see how he's going to handle it.

But we ended up creating this organization because we had to do something. And the lesson that I learned was in organizations that are

that large, that are that established, you're really trying to build that privacy framework as you're moving. And it was hard because everybody thinks their—the core mission at CAT, Inc., is building machines and selling machines. And it's different from a financial industry. It's different from a hotel where you are facing a customer. And the pitch for protecting privacy is more easily translated into: This is great customer service; this is what distinguishes us from this brand. If we lose their data, they may go to another hotel, they may use another credit card, they may use another bank.

Here, when we have systems that, on the manufacturing side we have a system called Product Link, which takes information from the machines all over the world and sends them back to CAT, Inc. Well, for that we use that system to monitor the machine performance. At CAT Financial we use the system to monitor, to shut down the machine or slow it down if you haven't paid your bills on time. But there are privacy issues with that. There are information security issues with that. There are state secret anti-mapping laws in certain countries that can't allow mapping coordinates to be transmitted outside of certain countries.

So it wasn't just privacy that we tried to do. I got my bosses to broaden the concept of it's not just privacy, because what I learned was privacy triggered HR. You say privacy, they think HR issue. But it was really information management, information government. It's data security. Talking to them about particular processes and treatments that we have that we don't even patent because they're so sensitive to CAT that we don't want people to know about them.

And then the question is: Well, how do you protect that information? I don't know. How do you incorporate a data loss prevention system in a worldwide system of e-mail in a way that doesn't violate Belgium law or a provision in Belgium law that says that correspondence is confidential and it's punishable by criminal law, including—and you know, you have internal attorneys that might interpret that as including correspondence through e-mail. How does that jive with an online data loss prevention tool where you're trying to actually protect the company from loss of information?

What are the privacy considerations that we had to figure out when trying to implement a fraud solution system to look at our vendors and whether they were double-charging us and whether our vendors were related to employees?

Well, we had to go back to the privacy policy. Fortunately, we had one. Well, fortunately we had several that said different things. And so fixing that. But it's all a manifestation of business moving fast and privacy not being a consideration.

So then I moved to CAT Financial, where really the lion's share of the privacy issues are within the CAT, Inc., enterprise, because we're a financial institution. We don't do consumer lending. Our operation leases are sales contracts, which specifically exclude using the equipment for anything that would cause us to fall under consumer lending.

But, we have sole proprietors, sole proprietors all over the world. Our largest customer in Germany is a sole proprietor. Well, that's technically a consumer. And his information is personal information.

So the challenges we face are, and they're laudable goals in terms of protecting personal data, but we run into these goals and policies when we try and create greater efficiency. So CAT Financial has got thirty-four international subsidiaries, does business in more countries throughout the world than CAT, Inc., does.

Well, each of those subsidiaries may have—several of those subsidiaries have their own intake and origination platform for creating a loan. Well, those are all disparate and different. And so how do we get a view of one customer back at headquarters in Nashville? Well, we're trying to implement one solution and one system.

How does that work in terms of international data transfers from a region that is, like the European Union, which is fairly conservative, or at least process driven, some might argue burdensome, in its approach to deploying unified systems that collect and aggregate information and send it back to different places?

So trying to figure out those efficiencies, trying to figure out how we interact with our dealers who are collecting the personal information and what obligations they have. Because a customer doesn't know that. They see a CAT dealer and they go in and think that they can finance it. But they don't really understand that that CAT dealer is not our agent in a legal and technical sense. But if they lose that information, then it's really the CAT, Inc., the CAT Financial brand and reputation that's on the line.

So what do we ask them to do? If we look at our sales and service agreements, which is the CAT, Inc., agreement with the dealers, or the retail finance agreement, which is the CAT Financial agreement with the dealers, there's very little information that incorporates privacy.

And then again, you're got worldwide organizations creating projects to try and harmonize information, and people are thinking about the stuff every day.

And so what we've actually done is taken what we've learned from the government in terms of privacy threshold analysis, privacy impact assessments and finding choke points where we can get up to eighty percent of the work. And that would be we've got a Six Sigma process and so we're trying to get incorporated. Every Six Sigma project has to have

some sort of privacy threshold analysis done. Does this impact customer information, personal data? Will it be shared? At least getting that on the front end.

We also have a new project initiative that everyone has to go through when they have a new system or a new project. And so those are two choke points where we can put in a process for people to be conscious and raise the visibility of privacy and be conscious of those. But it is hard. And I think the challenge that we face every day, really, is how do you take a global company that has a parent company with kind of this mission statement, this policy on data privacy, but how do you implement it in a way that is practical for the business and is lawful in the countries in which you're operating but doesn't slow the business down? And all over the world. Can you do that? And can you do that without adding cost or without adding head count? And those are the challenges that you kind of face every day, or that I face a lot in the privacy perfective.

(Applause.)

PROFESSOR REIS: Well, thank you. I'm sure that will generate some interesting discussion in a little bit. Our final speaker on this panel is Professor Peter Swire. Professor Swire is recognized internationally as one of the preeminent scholars in privacy law. He is a professor of law at the Moritz College of Law at The Ohio State University. In 2009 through 2010, Professor Swire was a Special Assistant to the President for Economic Policy serving in the National Economic Counsel under Lawrence Summers. And from 1999 to early 2001 he served as the Clinton administration's chief counselor for privacy. And his talk, bringing some of this together this morning, and like a true academic does have a hyphenated, or rather a colon, in its title. Self-Regulation and Privacy: The Importance of a Credible Threat of Government Action.

(Applause.)

PROFESSOR SWIRE: Thanks, Leslie. It was just so interesting listening to Mary Ellen and Renard tell their stories. Can you imagine getting all of DHS to do something or all of Caterpillar? across the whole world? And that's what they woke up every morning trying to do. And it's a big challenge. My thanks to Leslie and David Sorkin and John Marshall Law School for setting up this program. It's been a really interesting two days. I'm going to first ask, for the people who work, who aren't students anymore, how many people have privacy as a sort of significant part of your work these days? A lot? Not too much?

(Show of hands.)

And of the people who work, how many didn't put up their hands but you're working right now, it is not so much what you're working on?

(Show of hands.)

The first group is privacy is part of your work when you go out and work every day.

(Show of hands.)

Privacy is not part of your work really when you go out and work every day.

(Show of hands.)

Okay. So most of the folks here are not mostly living privacy day-to-day. And so we can have acronyms that could just like glaze your eyes, et cetera. But let me, with that as a sense, say in the privacy discussions I think we're often caught between optimism and pessimism.

So here is some optimism. Optimism is Mary Ellen is making sure across the agency that these things are being done the way they're supposed to be. And pessimism is we find out there are warrantless wiretaps happening in the National Security Agency.

MS. CALLAHAN: Not by DHS.

PROFESSOR SWIRE: Not by DHS. And we hope not by NSA today because there were some like exposes. But in 2003, the Justice Department said there's something called national security letters, which are the FBI can go without a warrant and get the detailed phone records and other things from people. And they testified in Congress that it was being used dozens of times that year. And then we got an IG's report about five years later and it turned out the number was over 100,000 that year. So that seems like more than dozens.

And so we see a gap sometimes between what's stated and what's done and we're left with this pessimistic worry that things are happening we don't like.

We can have optimism about, Renard talks about the Six Sigma's process where part of quality is quality when it comes to management. And we also can see in an optimistic way that there are professional groups, like the International Association of Privacy Professionals, it had 150 people in 2000; it went over 10,000 members this year. And so we

have a cadre, we have a trained group of people like Renard, very impressive and able to explain to all these business folks who never thought privacy was part of their job, here is what we do that's quality.

And that's happening throughout organizations globally and I think that's very optimistic. But then you can read the Wall Street Journal's exposes about technical practices of cookies replenishing even when you delete them and all the rest and you can get pessimistic.

And so somehow we're trying to figure out, as this information wave flows through us, when to feel optimistic and say "This is the way to go" and when to be like, "Oh, no, it's really as bad as we feared it."

Some of that optimism and pessimism comes upon whether we should have the markets or the government or something else handle this. So in Europe, as we heard, there is the European Union Data Protection Directive, a comprehensive set of rights for the individual that applies to all your personal data. And it's implemented by government agencies. It's a great big directive that we've had since the 1990s. And this year in January they proposed a new draft regulation which would be a unified law for all the, whatever, 600 million people in the EU, and it goes substantially further, much stricter, to sort of a complete system for rules for how you handle personal data.

And if you're Caterpillar or all the other global companies, or an Internet company in the U.S., you've got this set of government rules being run by the people who write and enforce government rules. And that's sort of scary if you're in business, because you think they might not be perfect every second.

Another optimism is maybe we can just think the market is going to take care of it, right? So we have a lot of faith in the United States, depending on our mood and what part of the election cycle we're in, we have a lot of optimism in the market. But when it comes to privacy practices, we hear things like Wild West; we hear things like apps for our phone, you know, Angry Birds tracking your location or whatever it is. Like, what's that about? Your phone is a tracking device and perhaps hundreds of different apps that know where you were yesterday.

And then what are they doing with that? And there are no laws on that subject. And that seems a little scary.

And so an answer, too much government sounds like too much government bureaucrats, too much market sounds like who knows what those guys are doing. An answer that's been overwhelmingly tempting in the privacy debates has been what they call self-regulation. And I want you to get optimistic for a minute and then I'm going to get more pessimistic.

But here is the optimistic view, which is, that responsible companies will get together themselves or with other companies and they'll figure

out good practices. They'll figure out standards. They'll define what's okay and set a norm so everybody knows what they're supposed to do.

And let's get more optimistic. In the Federal Trade Commission where Renard has worked, where Mary Ellen has practiced in front of, they have this unfair and deceptive practices law. If you make a promise and you break it, it's your promise, self-regulation, but the government is going to enforce it. And they can get consent decrees. And consent decrees today exist for, hmm, Facebook, Google, Twitter, Microsoft, MySpace. Most of the major, huge are all under consent decrees. And they've defined their own practices and now they're enforceable. And so self-regulation is this way, where the industry comes up with the standards and then they get stuck with them, but maybe that's better than the government writing a bunch of rules. So that's the optimistic view of self-regulation

The only thing wrong with it is, historical experience shows that it doesn't work. And that's what my talk is about. So I wrote a paper on self-regulation in markets and government regulation in 1997 for privacy. So that's a while ago. The Internet had been commercial for three years at that point. And they were really proud because, I don't know, there were 50 million on the Internet or whatever it was.

And it went through the reasons to think self-regulation might work, because we get this pressure on industry to do good things and then they be held to it, et cetera.

I was asked to testify in front of the Senate Commerce Committee this summer and went back and looked at the history. And that's part of what I'm going to walk through. And the history was that self-regulation does work, it works during those moments when government is really focused on it. And it goes something like this, okay. Think about if you're just sitting there and this is an issue you know nobody cares about, and you're meeting with your clients, you're meeting with everyone, and somebody says, "Let's come up with our self-regulatory promise. Let's promise not to sell our data to third parties because we don't think it's right for us to grab data from our website and then sell it to all these other people."

And the other business people are saying "Well, we make money selling it and we share with other people, just like we used to share catalog lists and stuff." And you go around the room and saying "Do we want to tie our hands here?" And the answer goes something like this, "We really don't need to do this right now," right? That's the business decision, that's what's happening around the conference table.

Now, let's imagine, however, that your CEO is being called to testify in Congress next Thursday, right, and that your general counsel was hauled in for another meeting where he or she had to say stuff. And

they're saying, now, they come back from that meeting getting ready for the testimony and their statement goes something like this, "We really better do this or Congress is going to do it for us. If we don't have a good answer, if I can't say something good in my hearing next week, we're going to get hammered. We better come up with something."

And the history of self-regulation is when the hearings are happening, when the FTC is having workshops, when the President is making statements about it, we've seen very substantial efforts by industry to do stuff. And when the pressure comes off, the programs wither away.

So I'm going to talk about the sort of first wave of privacy stuff for the U.S. in the '90s, talk about the history after 2001 and especially the attack of September 11, and talk about the second wave we're in today. And that's the sort of structure.

So the first wave in the 1990s looks something like this. That's when we wrote the HIPAA privacy rule, you remember that? So I was the White House coordinator for the HIPAA privacy rule. It was fun and easy. We had proposed rules in 1999, went out for public comment, and got back 53,000 comments. And so fourteen agencies, seventy people, we worked on those comments and got the final rule out. And the statement we got was "Thanks"—I hear from a lot of doctors—"before HIPAA happened there were no national privacy rules to speak of, or national data security rules."

HIPAA happened because at that moment we were going from paper reimbursement for federal reimbursements to you only get paid if you submitted electronically. And the basic idea of HIPAA is if we're going to send all the bills through all the insurance companies in electronic form, we ought to have some data governance around that. Having all that electronic flying everywhere, with no privacy, no security, was a bad idea, not the Hippocratic oath. You can have all sorts of views about whether it makes sense or not, that was the rule we came up with. We came up with Gram-Leach-Bliley, the banking privacy rules, you get your notices.

COPPA was a law, the Children's Online Privacy, you shouldn't have cartoons that say, "hey, kids, tell me what kind of car mommy drives and what she went to the grocery store for this week." You shouldn't have kids being used as spies on their family.

We passed laws on these things. But most of the 1990s was self-regulation. Most of it was the Federal Trade Commission and the Department of Commerce, Bill Daley and President Clinton, saying "Industry, come on, come up with something plausible here for these new websites, have a privacy policy and stick to your promises. And if you do a good job, we're not going to write a law."

So the Clinton administration never came to the point where they said Internet privacy should have a law. They said, "Let's go, and let's see what we can get out of industry effort."

And in 1997 there was the first survey of how many websites had privacy policies. And the answer was about twelve percent of commercial sites had privacy policies. Two years later, with this "Come on, guys, do it or we'll do it for you," two years later that twelve percent was up to eighty-eight percent of commercial websites. So that credible threat, "Come on, we're really going to do this, the Internet is happening, you better help us," got major effort out of industry. And so that problem, if not solved, became pretty much the norm.

And it got locked into law in California a few years later. So if you have a website that's commercial in California, you have to have a privacy policy up. And they're making it right now in California where you're going to have to have a privacy policy for your apps as well.

But that was a big self-regulatory effort and it moved the industry faster than a law would have done. I think it was a big success.

Part of what it showed was that self-regulation is not all one thing, it's not just the self, where the industry does it itself, it's like separation of powers. So remember, in separation of powers you have the legislature who writes the rules. In this case the companies were writing their own rules, or the industry groups. You have the executive who can bring enforcement and write regs. That was often the FTC. And then you have the judiciary that would sit there and adjudicate at the end.

So what we saw from self-regulation is, it was industry did come forward with a bunch of promises and then the enforcement happened by real live agencies and we got substantial progress.

What happened next? Well, what happened next was privacy fell into eclipse. And one reason was the change in administration, but a bigger reason was 9/11 happened. And in 9/11 we had security as a huge deal. We had information sharing as the way we were going to connect the dots, find the terrorists and keep ourselves safe. And the privacy discussion really sort of went away from most parts of the privacy discussion for a number of years.

Here is what happened on the self-regulatory efforts that were going at the time. So there was one report issued by the World Privacy Forum, and they said, summing up the next seven or eight years, we now have repetitive specific tangible examples of failed self-regulation in the area of privacy. These examples are not mere anecdotes. These were significant national efforts that regulators took seriously.

They said, looking at the history, the privacy self-regulation organizations were loudly promoted despite their limited scope and substance. And so I'll just give a couple of examples. One group from the '90s is

something called the Individual Reference Services Group. This is the group for Lexis, Choicepoint, the people who sort of keep your social security number and identity information. They were announced in 1997. They made a deal with the FTC about how good they were going to be on all this stuff. They closed the group in 2001. Pressure was off, the group closed down.

And the Federal Trade Commissioner, Julie Brill, has recently said we've really got to go back here, there's a lot of practices in the data broker industry, but the self-regulatory group had disbanded in 2001. There is a group called the Privacy Leadership Initiative that was announced in 2000. Privacy was a hot issue? They announced they would spend $30 million to $40 million to support self-regulation. But because the issue soon faded, they closed that group in 2002. It went from $30 million or $40 million, huge effort, major issue, to close down.

The Online Privacy Alliance Christine Varney helped to form was at the center of the debate in this period. Its last reported activity, according to its website, seems to have taken place in 2001.

These were the biggest self-regulatory groups. They were in the newspapers, they were in Congress, and they were making a big deal. They closed down.

One more and then I'll stop. The Network Advertising Initiative was going to be the way to handle online advertising things; it was trumpeted when it was created in 2000. But by 2003 the NAI's membership was down to two members. So the online advertising industry's self-regulatory effort had two members by 2003. Today it has about 100 members. It's highly active, has a very energetic executive director; but we're back in a privacy era, not the era we were in in between.

So if you want to believe in self-regulation, you can believe in it; but it didn't work when people turned their attention to other things. Where are we today? Today we're in what I've written about as the second wave of privacy, global privacy protection. In fact, we're going to have a conference at Ohio State in November called The Second Wave of Global Privacy Protection. Here is some of the stuff that's happening these days. How many people were on Facebook five years ago?

(Show of hands.)

Wow, we've got some early adopters here. How many are on Facebook today?

(Show of hands.)

Pretty much like, if not, everybody, and then at least some member of your family tells about you even if you don't say it yourself. Okay. So in five years we've gone to 800 million people.

How many people don't have a mobile phone today?

(Show of hands.)

We've got two, three. Okay. Ten-fifteen years ago most people didn't carry them and nobody had a smartphone. So when it comes to mobile, right, this is a tracking device, right, there's data about where you've been and the cell towers triangulate and know where you've been. In the history of human behavior, we did not have tracking devices on us, today we all do. Just worth noticing there might be privacy issues there.

Online ads have come back. So there's a study that came out earlier this year. Of the 100 most popular websites, it found that twenty-one out of the 100 place 100 or more cookies onto your computers when you visit them. You go there once; you get over a hundred cookies. And eighty-four percent of the cookies are by third parties, which suggests an enormous ecosystem, which exists about how the data of your Web browsing is going everywhere. So you're on social networks and your mobile phone and you're on online ads.

And then also along with all these technical changes, the EU has its regulation, and some small countries like India and Korea and the Philippines, most of Latin America, Mexico, Canada, all have privacy laws, which they didn't have ten years ago.

So we have global laws. We have the EU ramping up the effort. We have massive technological change happening and privacy is back. And you can measure it in hearings on the Hill, you can measure it in President Obama giving speeches on the subject, you can measure it in the do-not-track efforts that are being done in a standard setting organization.

Have people here heard of the do-not-track debate? Is that a familiar thing? Not really. Okay. Have people heard of do not call, right, they don't call, you've heard that, right? Okay. Do not call is like they won't call you at home if they follow the rules. And we have a national law. That was such a popular regulation that President George W. Bush held a Rose Garden ceremony to announce it. That is a reg that is widely beloved across many parts of our domain.

So if you think you should be able to opt out of people calling you, maybe you should be able to opt out of being tracked when you're on the Internet. There's a sort of sensible thing. The name is absolutely wonderful, do not call, do not track, who can be against it?

Turns out knowing how to create do not track is really complicated. The industry groups, advocates and others are in the W3C standard pro-

cess. And there is this big effort to see what will happen of it. We don't have a law on the edge of being passed, but there's a big effort to do this.

So here we are today and we're seeing self-regulation coming back. We have the advertising agencies doing things. We have a lot of new industry statements for self-regulation. And it's really, really tempting, because we don't like big government bureaucrats telling us in America what to do. Technology moves fast, how the heck are the bureaucrats going to write rules. If you don't like HIPAA for health care, how are you going to like anything like it for the Internet?

All that makes a lot of sense. And what I say back is, I've been skeptical and cautious about regulations in this area for years, did not favor an Internet law in the 1990s, thought we should move forward with the industry efforts. But we've seen the history. And the history is there's a bunch of attention and a bunch of energy when the issue is hot and it's cool and it's on the front pages. And then industry basically plays out the clock. Basically what happens on the industry side is they say, "We think this will fade." Maybe there will be a new Congress or President next year. Maybe some other problem will come up and the attention will turn to some environmental disaster or something. And so if we can just sort of hold off the legislation, we know the drill, if we get through the next two years, there won't be laws and we get to keep doing what we want to do. That's what we saw last time. It's what's happening right now.

And it was sort of interesting. This was my testimony in June in the Commerce Committee in the Senate and you had senators saying, "These are very new issues. We really should give industry time to address them and industry is responsible and they should be able to do self-regulation."

My answer back was "Well, we've actually seen that and it didn't work." And they sort of didn't know what to say next.

And so I think you try to learn from history so you don't repeat it. Legislation can be wildly wrong. I have a bunch of criticisms that I'm writing up about the European Union's draft regulation right now. The fact that it's legislation doesn't make it right. But I think we have enough experience from these industry efforts to say if there isn't something that gets put into place and locked in more successfully, then we're going to see a next round of disturbing behavior, tracking behavior, sort of lack of consumer protections.

And so in sadness, rather than out of enthusiasm, I've come to think legislation in this area makes sense. The administration has supported that, a very sort of modest bill that's not European in style. And I think that should give us, I think, a little more reason for optimism than saying that it's all going to be okay if we let industry do it itself.

So thank you for your attention, we'll look forward to the questions.

(Applause.)

PROFESSOR REIS: In hearing the various perspectives, and especially the sort of historical perspectives coming from both Mary Ellen and Renard, gets me thinking about some of the relevance of the principles underlying privacy protection. And I'd like to ask the panel about whether you believe that there is still relevance in what many of us learned as core principles of privacy protection.

Since the 1960s, late 1960s/early 1970s, there have been efforts to articulate a core set of principles for privacy protection. And depending on who the author is of these particular sets of principles, there are either eight or five, or a number of them, and I want to just, in deference to Renard, list off the five principles that either a self-regulatory mechanism or perhaps legislation would, at least under the sort of classical theory of privacy, take into account and see what you guys think of it.

These principles for any entity that collects or uses data would start off by taking into account providing some sort of notice or awareness to the data subject.

The second principle is choice or consent, giving some choice or method of consent again to the person whose data is being collected.

That some sort of access or participation, that's the third principle that would entitle that data subject to have access to that information, to know what information is in this collection of data.

And in some form of integrity or security provisions that the data collector must undertake.

And then the fifth principle, some sort of enforcement or redress.

And in the current state of affairs, shall we say, there has been a lot written on the lack of relevance today for two of those principles in particular, choice consent and the access and participation principles. I'm just wondering if you think these are good ways of thinking about privacy, or not?

MR. FRANCOIS: Well, I'd add one more to them, because these are actually the policies that we have in our enterprise policy on data privacy, these are the concepts that our company tries to, on an enterprise level, uphold. And I would add the onward transfer concept, because I think that that's very important for us.

And I look at these, as these are just good business practices. It doesn't affect our bottom line to tell people how we're going to handle their data, what we're going to do with their data, to try and get their consent and provide them access to it and have accurate information. I

mean, we're a financial institution and we don't want to pull credit bureaus on people who are no longer with companies guaranteeing debt. It's a waste of our time. It's unlawful under the Fair Credit and Reporting Act. And there are a host of reasons, business and corporate citizenwise to do it.

And also the way we look at it, the reason we say onward transfer is because that data is our obligation no matter who has access to it. And so if we give it to a third-party vendor and they lose it, then that's our obligation, that's our data in the regions of the world where we operate and it's inexcusable to say, well, we gave it to somebody who was incompetent. And so that's what we do.

The other thing that I would say that is a challenge is having a realistic concept of harm. Because we go around and around. And I've done this on the CAT, Inc., side, I've done this on the CAT Financial side with some of my colleagues in Europe, is talking about the information and its impact on the individual. Like, yes, I know, according to the black letter, the sales representative of the customer's name and business telephone number and business e-mail address is personal data, but what's the harm if that data is lost? You know, the purpose of it is to be publicly given because it's on a business card. And so having those conversations and having a little bit of clarity in terms of how you approach those, well, maybe it is technically a violation, but is that someplace where we can assume a little bit of low risk?

So I think the principles are great. I'd add that one. But I'd also add in this concept of looking at harm, not as an excuse, but making sure that we want to be reasonable in what we do. But we also want to make sure that we're taking care of individual citizens and the rights that they have.

MS. CALLAHAN: So I'd argue on the FIPS, that they absolutely are very relevant. And even if notice and choice may mean slightly different things in a Facebook era than they did in 1974, they're still very germane, and they're the lens through which we should think about privacy and how to implement privacy, right? Privacy by design is the new sexy term.

Well, what does that mean if not in the framework of the FIPS? And you rattled off the FIPS and Renard added the onward transfer. At DHS we actually have a pretty robust FIPS framework that has eight. We're among the eight people. And the two that we added I think are useful to think about, private and public sector, which are purpose specification, right, so why are you collecting this information? And that is actually integrated into the Department of Commerce's consumer bill of rights, that concept, not expressly but somewhat like that. And then use limitation relatedly in terms of limiting the use of it. And then there is the

transfer element and accountability, which I had talked about as well, which is somewhat related to the redress point, which is, of course, one of ours as well.

But I think you've got to have a framework in which to operate. There may be different emphases, depending on if you're talking about consumer-facing, business-facing, and that sort of thing; but it's got to have a rubric, otherwise it doesn't hold together.

PROFESSOR SWIRE: So the fair information practice principles, there are a lot of formulations. I think what I heard here is you're teaching your whole organization privacy and they don't do it most of the time, you need this structure. This is the way you communicate it out to the components and you need to have some structure.

And so I have two books coming out this fall for the International Association of Privacy Professionals, the foundations book, so the test for the first foundations certification, and then a book on U.S. privacy law.

And if you're going to try to communicate to students, to people working in your organization, you need something that's not forty pages long. And so saying you have to tell them what it is, you have to give them some choice about it, you have to let them have access to it, you have to keep this data safe and you have to enforce, and then you add maybe some good data quality and don't use it in surprising ways, you have a chance to get that out to your organization. So that's the first thing.

What's hard is that that doesn't get at a lot of the next round of problems. So we live in a world today where the number of censors is going way up, right? Everybody carries a camera today, you all carry a tape recorder today, your laptop can do sound recordings if you want to while we're sitting here. And there are cameras everywhere and the rest.

So with the amount of data being collected, it's just going through the roof. And saying you have notice about that doesn't capture whether this much is okay or this much is okay or this much is okay. And we'll need other ways to talk about what's in bounds and what's not in bounds, but you need the basic structure to be able to talk to people about this stuff.

MR. FRANCOIS: Well, and to add to that point, I think the way you phrased it is great, because some of the challenges that you have, particularly I think in government, in corporations, is it's a noise factor.

And so I had a meeting the other day with some people and we were talking about one of our initiatives on export control and we were talking about the noise. So for our subsidiary in Germany, they're getting, the compliance person is getting information from their managing director,

the vice president who is in charge of that subsidiary office. The senior leadership from the CAT Financial, they're getting information from me and they're in-country attorney about certain things that we all think are important. And then you layer on to that what comes from CAT, Inc., and the senior management from CAT, Inc., that has to be cascaded down to them. And that's just all work and not to mention the personal stuff. And so it's how do you filter—and the tendency is, I don't know if this is true in government, it's certainly true at CAT, Inc., is: This is really important, so we'll not have a thirty slide PowerPoint presentation, we'll make it eighty-five slides.

And so there's so much noise that you have to have something to communicate it in a way just to maybe get eighty percent at a corporation level to get people to focus on. I tell them we should go back to simplicity. Limit the slides, repeat things over and over again. And they may want to jump out of a window because it drives them crazy, but at least they will jump out of a window repeating what we want them to repeat.

And so having those concepts, I think, can be helpful as you're trying to really educate and establish that foundation so you can address more sophisticated issues.

MS. CALLAHAN: So I can visualize the headline: CAT, Inc., Encourages Defenestration.

PROFESSOR REIS: Well, thank you all. I know we've got time for at least a few questions.

FROM THE FLOOR: A question for Mr. Francois, which you raised in my mind when you mentioned good business practices. And in corporate America, is there an area where business is cooperating as to relevant best practices thereby saving time and money? So if you're in Peoria at Caterpillar, John Deere is in Moline, do you talk to your counterpart at John Deere and find out what they do, adapt it to your business? Or it doesn't really work that way?

PROFESSOR REIS: And if I could, before your answer, let me repeat that for the purpose of the tape. I believe the question is: Can industry members cooperate in terms of defining or setting up best practices?

FROM THE FLOOR: That's right. In ways that also save money.

PROFESSOR REIS: In the interest of money saving sufficiency and all of that.

FROM THE FLOOR: And developing best practices.

MR. FRANCOIS: That's a good question. And in certain areas I think they can. And in certain areas I think it would be very difficult.

We are undergoing at CAT Financial a compliance Six Sigma project. And we've reached out to Deere, we've reached out to Volvo Finance, we've reached out to Louisiana Pacific. And so I think there are areas where you can do benchmarking that are probably not in core mission critical company areas.

But if we wanted to reach out and do benchmarking and develop best practices for how to develop a backhoe, that probably isn't going to go very far. But I think particularly there are opportunities in that, specifically for places like CAT and Deere, maybe even Komatsu, I'm not sure. And it's one of those things where I think it's a little bit different because we are manufacturing companies as opposed to kind of the social media companies. So that pressure, you see some cooperation and collaboration in like the online, the Network Advertising Initiative. I think manufacturing companies are just a little bit behind because they look at it and, say, well, the HR folks will handle that. And so I think coming from looking at more the information governance, I think there are opportunities to do that.

I think individually several of the companies are really trying to do the right thing. And it may be one of those things. Like I feel bad for my colleague who is back in Peoria, who replaced me after I moved to Nashville, I mean he is an army of one, who's got no paralegal and, you know, whenever there is austerity measures, it's we clamp down on outside legal work. And it's overwhelming for him. And so I'm sure if he had sufficient resources to do that and had the time to reach out, he could build those coalitions and they can do those things. But privacy is not, when you get down from the major leagues and the AAA level of the issues that you face, which are more customer-facing and retail, you really are fighting, sometimes shouting in the wind, to raise the consciousness of privacy issues.

PROFESSOR SWIRE: So one thing that happens is there is this professional association that really didn't exist ten years ago, the IAPP, and so there is training materials and stuff.

Another thing, there are the PCW's and Accentures of the world that provide that service. So they get to know for lots of clients.

And some of the law firms do that. I worked with Morrison & Foerster for several years where they mostly did financial services. So they could develop expertise that different banks then can draw on. So there's ways to get expertise, not necessarily all in-house, where you get help on that a lot of the time.

FROM THE FLOOR: What we've heard this morning is an overview of policy and it's excellent. But where I have a problem picking up policy is with all the rights that are formulated along with the researchers and prohibitions. How has the public got some idea of what all these things are? And I guess some comments may be on how we spread this information out so that we don't get bogged down with people just not knowing where this is going.

PROFESSOR REIS: I think that's a wonderful question. The question I think relates to how do we translate all of the things that we have been talking about, sometimes in legalese, sometimes using our abbreviations, to the general public to understand not only the breadth but also the depth of the concerns that we're trying to grapple with in terms of either self-regulation or government regulation.

MS. CALLAHAN: I think that's exactly right. And I think it's a hard question. And I think it's one that private sector/public sector deals with.

On the public sector, again, we have a requirement to print these privacy impact assessments and the system of records notice which are so archaic and so Byzantine. But the point is to be transparent. But what does that mean to you and me and how does that intersect? And I think that's a very tough question, because you want to be full disclosure, tell everything. Going to Renard's point is, you know, okay, is it eighty-five slides, is it a privacy policy that's twenty pages long. That doesn't help anybody other than the outside counsel. I mean it's just a CYA and, okay, all this.

But we were debating what dothe FIPS mean. And that notice provision to get to that right level of understanding what it means without being icky, scary, is a really tough balance. And I don't think it's been struck yet.

PROFESSOR REIS: Any other thoughts?

MR. FRANCOIS: I don't know. I mean maybe some of it is in the historical context. I mean you look at the European countries that have the most stringent views on data protection and those tend to be the countries that had issues in World War II with secret police and spying. And I think awareness and sensitivity to it might be part of their culture. And I'm not trying to say it negatively, but I don't know that we've had that concern or that experience in this country that makes that concern so pervasive as a part of who we are.

I mean I think we can say, like Mary Ellen said, there are privacy policies, there are things you have to click and scroll. The FTC tries to

educate consumers in every way, shape, form, speeches, interviews, websites. And then on some level I think it's just up to us as individual consumers to educate ourselves and to educate others. And maybe even in our own capacities. I mean, one of the things that we do is we tell people if you have a mobile device—we did a presentation at work—this is how you lock it. So that you don't leave your iPhone sitting on your desk, because you might have, and our hook was, you have a work contact. You might have the president of our subsidiary's mobile number. You might have a work e-mail. And so you have an obligation to work, but also individually, to learn how to secure that. So we kind of took that moment to do a little bit of a public service announcement. And I think maybe taking those initiatives helps to make one step at a time, one person at a time.

PROFESSOR REIS: And Peter, can I give you the last word.

PROFESSOR SWINE: I was just going to very briefly. There is some good reporting on this. Julia Angwin at the Wall Street Journal has a series that I think was nominated for a Pulitzer Prize last year called "What They Know." And so you can go to the Wall Street Journal, you have to pay for it, it's behind a pay wall, but the Wall Street Journal has given very detailed but readable stories about what's done.

Robert O'Harrow wrote a book a few years ago called "No Place to Hide," and his reporting was also nominated for a Pulitzer Prize.

So "No Place to Hide" and "What They Know" are two places where reporters trying to speak English have written about this.

PROFESSOR REIS: Well, given that Professor Sorkin is giving us the evil eye, I would love to offer some more discussion, but I think we are at the end of our time. I would like to thank our phenomenal speakers—Mary Ellen, Renard, Peter. And of course, thank David Sorkin for organizing this phenomenal, wonderful, terrific conference.

(Applause.)

PROFESSOR SORKIN: Thank you, Leslie, and thank you to the panelists. We're going to take a brief coffee break before the next session. Please join us down on the third floor for some light refreshments and then we will resume at 10:30 for Section IV.

(Whereupon a recess was taken.)