UIC John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 4 Article 12

Spring 2015

Legal Problems in Data Management: The Impact of International Data Restriction Laws on U.S. Companies, 31 J. Marshall J. Info. Tech. & Privacy L. 609 (2015)

SESSION SIX:

THE IMPACT OF INTERNATIONAL DATA RESTRICTION LAWS ON U.S. COMPANIES

MODERATOR:

WILLIAM MOCK
PROFESSOR, THE JOHN MARSHALL LAW SCHOOL

PANELISTS:

GARY FRIEDLANDER
VICE PRESIDENT AND DIVISION GENERAL COUNSEL,
TRANSUNION LLC

DEVEREUX CHATILLION
PARTNER, CO-FOUNDER, CHATILLION WEISS LLP

ALISON HARKINS
OF COUNSEL, MCKENNA STORER

PROFESSOR WILLIAM MOCK: Good afternoon, everyone. Thank you for being here. I'm Professor William Mock from the John Marshall Law School. I was one of co-founders of the Journal that is sponsoring this symposium some few years back, and I'm delighted to be the moderator for our next panel, the panel on The Impact of International Data Restrictions on U.S. Companies.

I'll briefly introduce our three panelists and then throw a few questions at them. We'll have a bit of a discussion going, and well make sure that as you become interested and wish to join in, we will save some time for audience participation and audience questions on these topics.

Our three panelists I think will be well qualified to address these issues.

Dev Chatillon, who is the partner and co-founder of her law firm that deals with copyright and trademark. She graduated from Harvard and from NYU with a law degree and has done immense work in copyright and trademark strategic positioning, risk management, litigation advice. And I would say, to me, since I want to keep these introductions short, her greatest claim to fame was probably that she had the nerve to write a law review article about Sherlock Holmes.

(Laughter.)

Actually, it relates to our topic, because it had to do with a public domain.

Next in line is Alison Harkins from McKenna Storer, in-house corporate counsel for major corporations over the years, 3Com, NCI, Accenture, and a number of others. She handles a lot of international business transactions, including a great deal having to do with technology, cloud computing data, software licensing, things of that sort. She is a graduate of two rival schools, as I understand it. Arizona State for her bachelors and University of Arizona for her JD. I will not ask who she roots for when they play.

Third is Gary Friedlander, who is Vice President and Division General Counsel at TransUnion, has been for the last 16 years. I'd like to claim some credit for his successes, only because he was actually my student many years ago, and I'm always proud to see my students on panels and producing wonderful results in the world. He is very active in overseeing in-house counsel located throughout the world, U.S., Brazil, Canada, Hong Kong, and South Africa is the list I found, but I suspect there are others, and does a lot of the intellectual property work. For those of us in Chicagoland, he's also very active, having been involved with almost every major civic organization I could find in the City of Chicago, including just about every museum and public radio.

They are all experienced in dealing with international business transactions, international business ventures of various kinds, and with

the information law aspects that have become increasingly important. So I'd like to begin by asking them a question.

Most recently, there has been a lot of development in the European Union having to do with databases and corporate databases, in particular, and the right to be forgotten. How do you see that impacting U.S. companies?

MS. DEVEREUX CHATILLON: Why don't I start out with a little background for those who haven't followed this as closely as others.

This is kind of a slightly odd development. I'm sure you're all aware of the EU directive, which I just looked this up again so I could have a qubit. It requires all data about EU citizens to be gathered with notice, they be given a choice, they have access to it if you kept it securely, and that the data have integrity.

An interpretation of that in May 2014 by the Court of Justice of the EU expanded it to require search engines to allow consumers to file requests to have search results about them deleted if they didn't meet certain criteria.

The underlying case came out of Spain for a lawyer, I'm sad to say, who objected to the fact that a foreclosure notice, which actually was one of those paid advertisements that municipalities must put up when they are going to foreclose for lack of payment of taxes or payment of the mortgage.

So the Spanish newspaper went online. Google did its algorithmic searches. As you searched for this man's information, up came this foreclosure notice, and since he was a lawyer dealing with financial transactions, he found this disadvantageous to him.

He sued both the Spanish newspaper, Google U.S., and Google Spain. The court held in Google Spain, even though I think it's not actually incorporated in Spain, and, ultimately, it was decided, without going into too much gory detail, that the Spanish newspaper did not have to take down the foreclosure notice, but that Google did need to delete the search result that served that up as you Googled his name. That came out his exception in the EU directive for journalistic enterprises. That was held to apply to newspapers but not to apply to Google.

So Google has taken the position, and I can -- they had over 800,000 -- about 850,000, last time I checked -- requests for deletions. They deleted about a quarter of a million of them. They have a panel. They spend enormous sums of money on this, and it's very, very vague standards that the court announced -- are you guys looking for this -- which was, your deleted results, they were inadequate, irrelevant or no longer relevant or excessive in relation to those purposes, and in light of the time that has elapsed. Not an easy standard for private companies certainly to apply.

So I think for most companies, certainly for information companies

doing business in Europe, this now poses a puzzle. I suspect most of them are going to try to take on the journalistic mantle rather than the search engine mantle. One of the ongoing disputes, there has been some court action, some regulatory actions where Google.com, which does not delist pursuant to this, as a U.S. entity, should be delisting, whether this should be worldwide or just limited to the Google search engines in Europe itself.

MR. GARY FRIEDLANDER: So I'd like to just add a bit of a twist to this, okay, because I don't think the concept of right to be forgotten is all that new.

I think -- I think with the EU and a lot of the offshoots in the laws globally, most of the database types of laws are consent based. And I'm sure we're going to talk about this more on the panel, but it all hinges on consumer providing consent in order to collect the data and then the consumer's ability to basically say, no longer include me in the database.

So I think that right to be forgotten is there in a way, and, in fact, even in the United States, so I happen to be in the credit reporting industry, Fair Credit Reporting Act also states that after a certain amount of years, that that data falls off your credit report. I think where the right to be forgotten is going, though, with the Google case is not so much the right to be forgotten, but, honestly, it's erasing history.

MS. CHATILLON: Right to edit your own credit history.

MR. FRIEDLANDER: Erasing online history. So the history still exists. I kind of think some of this is, honestly, an offshoot of what we've seen with the Snowden fiasco in the NSA, right? I think we're seeing a backlash globally. We saw that in Brazil.

So after Snowden, Brazil's president Dilma Rousseff was very upset because we were spying on her and immediately wanted to rein in what the internet companies could do there when she realized the economic impact backed up.

But I think that's what this is all about. It's a backlash.

MS. ALISON HARKINS: You know, I think there is also a kind of element -- there is still a balancing act. Even in Europe, I think there's a balancing act, even about freedom of speech as well as freedom to media. I don't think it's just the media that has that right. I think there is a broader right, but that said, I think in Europe it's just a stronger right to have that information removed.

I mean, here in the United States, as you point out, Fair Debt Collection Practices Act, to take some other action, you might have some right, but you don't have a generic -- general right to go to a search en-

gine and say, I don't like that information; it's ten years old or five years old.

But I think if there's accurate information even in Europe that's, I think, a year old, that's not going to be removed. Also, a lot of the statutes that are coming out or cases that are coming out are saying that that is the case.

PROFESSOR MOCK: Is there a difference between the question of the right to be forgotten in a business context and the private context? After all, the United States, we now have movements to remove, for example, Venchur's websites, and that's a form of the right to be forgotten.

Do you see, perhaps, some of that social movement for protection of parties that are being attacked online or cyber bullying, forget me from all that, as well, that that may dovetail with some of the European business initiatives, and at some point we're going to have more of the right to be forgotten in this country.

MS. CHATILLON: I can start. We had a little bit of that already with some of the privacy torts. There's public disclosure of private facts, embarrassing private facts. Although, under the Communications Decency Act, most websites won't have the liability if users are the ones who are posting it, which is one of issues that has come up with the revenge porn and other issues along those lines.

We do not have in this country, for a variety of reasons, including the First Amendment, which does apply to search engines here, nearly as strong a privacy tradition as in Continental Europe. I think UK I would put separately for these purposes, and I think certainly if you turn to the Chicago Tribune, the Sun-Times and said, a citizen has a right to make you take down or delist your archives. They've gotten those questions. They get those requests routinely.

One of the issues we do face here and Europe is struggling with more explicitly than we are, is what happens when every obscure record that used to be buried in a Microfiche in a major public library is now on everyone's computer or everyone's desk in the entire country?

It's a very different scenario, the different balancing between private and public interest. But I don't see that we've actually made much movement to date other than extreme cases like revenge porn and other things. I'm trying to really grapple with that.

MR. FRIEDLANDER: Yeah, I don't think we are going to see a huge movement in this country toward the right to be forgotten. I think what you are going to see and what you are seeing is more push to get consumers access to the data that's being collected, particularly by big data companies. I think that's more likely where it's going to go.

Part of the reason I say that is Congress has been promising a little thing like national data breach legislation for the last, what, five, six years now, and they can't even move on that. So I don't see them moving on something bigger, like the right to be forgotten, particularly with big business law in Washington.

MS. HARKINS: Although there is right now, there is the consumer -- what is it, it's –

MR. FRIEDLANDER: The financial profession bureau.

MS. HARKINS: It's a new act, and it's -- the second draft has just come out. I think it's -- the Consumer Bill of Rights. That's it, the Consumer Bill of Rights. And it will have some penalties, although I believe that the penalties are only enforceable. It's not individual right of action. I don't know if that's going to change. I think that those are -- that act is going to certainly add some additional rights, perhaps, to consumers, and that is the federal government.

Now, whether that passes or not, I don't know, but certainly that's -- there is a lot of legislation that's being talked about at the federal level, and it's becoming more prevalent. It may over time pass, given the number of data breaches and other things. There may be at some other point a critical mass where people say, yeah, this makes sense.

Thus far it just has never before been successful for a whole host of reasons, but probably the most -- to me, the biggest reason is it's a capitalistic society. We tend to let --, let's let the court sort these out. We don't want to legislate these things. We don't want to affect business. We don't want to affect commerce, unless we have to, and there are other rights. There's other ways for consumers to advocate for themselves, but down the road I think that might change a little bit.

PROFESSOR MOCK: What we see in the comparative law is that every major legal system faces more or less the same problems. The interesting part comes when they try to address it in different ways. Some ways work better than others, and there are always going to be challenges at the borders, the overlap between the different approaches.

As far as the United States and Europe go and we'll talk about other countries in a few minutes, but as far as they go, the Europeans have taken a basic approach of establishing a right of privacy, the right to be forgotten, the right to privacy. This has been around for 40 or 50 years in one form or another. And there are, obviously, some precursors to that.

What is the United States' action that is the equivalent in terms of trying to preserve the interest of individual not to have shame heaped on them for their lives and not to have undesirable genetic information

and undesirable financial information floating out there in space? How do we go about it? How does that mesh at the border?

MR. FRIEDLANDER: Well, I think, to answer your question about how we are going about it, I think one way we're going about it now is the creation of a Consumer Financial Protection Bureau. They are all over this stuff, and that's their mandate. They are getting into all of these big data businesses now and asking a lot of questions and putting out a lot of rules for these types of protections. So I think -- I think primarily that's the way we're going about it.

PROFESSOR MOCK: Do those rules take the same approach as the Europeans, or is it more of a consent and disclosure -- how do they go about it?

MR. FRIEDLANDER: So one of the big differences between us and Europe and us and a lot of countries is we're an opt-out country. Most of the world is opt-in, going back to the consent base. So our approaches are different. It is opt-out.

CFPB is looking at, again, looking at accuracy, how the data is being used, how it's being distributed. I think you're going to see a lot more activism within that regulatory agency as more and different types of uses of this data become prevalent, particularly with respect to new technologies that are allowing -- that are allowing us now to be able to take unstructured data and combine it and analyze it and use it, something that even just a few years ago just was not possible. We just didn't have the computing power or the software technology to do that.

MS. CHATILLON: And I would also add to that, it's a little more historical. The FTC has been historically relatively active in this area. Again, it required notice to consumers that come after Facebook and Google and some of the biggies over the years claiming that it was an unfair consumer practice for Facebook to make these incomprehensible changes to their privacy policy and end up using your Facebook pages in ads for various different things that you did not consent to.

I gather from Gary, in talking before the panel, that switching a little bit to the CFPB, rather than the FTC, but it's a shock to most people in this country. It's real interesting when you say, there is no legal requirement that Anthem -- well, Anthem had HIPAA, but a lot of your -- Target doesn't have an obligation legally to keep your data secure. There are notification obligations of a breach, and there are general duties of negligence and other things.

There are some big class actions going on right now over big data breaches, but there is no federal statute that explicitly requires it, which seems kind of insane to most of us.

MR. FRIEDLANDER: Well, they do so -- they have to be compliant with PCI.

MS. CHATILLON: Yeah, but that's an obligation of the credit card companies, not of the consumers.

MR. FRIEDLANDER: Yeah, but they're storying the credit card information, so they need to be compliant with it. But the problem with PCI is --

PROFESSOR MOCK: What is PCI?

MR. FRIEDLANDER: Oh, I'm sorry, payment card industry standards. So thank you.

So PCI is -- PCI is a standard that's come up. It was developed by body, and it basically says that if you store credit card information, you need to keep it secure. The PCI document is just huge, and it requires companies to go through audits to be able to certify that they're PCI compliant.

It pretty much -- this is a voluntary standard, but it's pushed by Visa and Master Card, so pretty much if you're handling Visa and Master Card, you need to be PCI compliant. The problem is, that as we've seen with the Target and all these other credit card breaches, PCI isn't all that effective.

PCI 3.0 is coming out very shortly, and we'll have to see what additional factors there are, but, from my perspective, PCI is really a bust. It's a good step, but it's really not doing much too really protect consumers against breaches.

Honestly, if you look at the big picture, companies need to be doing what they need to do to secure their systems. That changes from year to year, if not sooner than that. But is there a cure-all? I doubt it.

MS. HARKINS: And let me just comment. On this, there are – I think the United States approach, which is very different than the European approach, is very sectoral, meaning that we spend a lot of time and our government spends a lot of time on HIPAA for health care data and GLBA for financial data. Then, yes, the credit card companies have their payment card industry standard. There's not as much on just a general privacy right, for example.

Now, Vermont has recently introduced a bill that would amend their constitution to add a privacy right. Now, I don't know where that's going to go, but certainly that would be the first state that I believe that would have added such a right to their amendment or into their constitution.

MS. CHATILLON: California has some stuff in their constitution as well but, again, hasn't really applied in this area.

MS. HARKINS: This is very general, yeah.

MS. CHATILLON: There is also interstate commerce to consider. It's not clear the states can have a role.

PROFESSOR MOCK: It is interesting, some of these examples you gave, especially you, Dev, about Target and then the Facebook absconding with people's photos and information for commercial purposes, those are examples in which, perhaps, a commercial misuse of a privacy -- private data, private information, or at least semi-private, because anything on Facebook is something you have already shared with the world at some level.

MS. CHATILLON: Not necessarily. You could have actually restricted it to your friends and family. I gave up, because I decided I couldn't master the privacy controls, but my kids tell me I possibly could.

PROFESSOR MOCK: Well, I wonder if that reflects somebody larger, though, because the European challenges a lot on the level of people get to find out about me as opposed to somebody's exploiting this for profit.

MS. CHATILLON: Yes.

PROFESSOR MOCK: And I wonder if that distinction reflects a transatlantic distinction.

MR. FRIEDLANDER: Do we need to agree here?

PROFESSOR MOCK: Or that our somewhat capitalist orientation orients us toward privacy rights within a commercial structure more than in the personal structure?

MS. HARKINS: Well, I think that that's -- and just on that note, there is -- for example, we are an opt-out for, say, things like e-mail, spam, that kind of thing; whereas, most of the rest of the world is opt-in. Certainly there are exceptions, if you've done business with somebody. Perhaps if you're sending spam or e-mails to somebody working in a business context, but the majority of the world is still in that framework, which, again, shows, you know the -- perspective here is more on,

I'd say, favoring business to a certain extent and certainly commerce. And it still provides the right -- you still have the right to opt-out of these various statutes, but --

MS. CHATILLON: I'm also -- I think there is a slightly different approach, and I referred to this before, and shows my media background as well, which is: given the First Amendment and sort of very fundamental commitment to the ability of each one of us to speak freely about the others until our speech runs into someone else's rights. We just haven't been asked protective and the expressive, as opposed to the commercial area of people's privacy rights.

It is not that the media in this country isn't getting deluged with people upset that now when they get Google, that 25-year old drug misdemeanor thing is coming up from a local newspaper. People are. It's a significant issue for a lot of the population. But under our current constitutional regime, the government can't really say much about that if the press entity or the expressive entity does not want to take it down.

PROFESSOR MOCK: This can come up also in the context, not long ago I was indulging one of my hobbies, which is genealogy, and I went down to ancestry.com and did some research and discovered that a certain pair of people in my family, my extended family, weren't married when they claimed they were.

(Laughter.)

And that led to an interesting discussion.

MS. CHATILLON: In case the more mundane levels and weird things sort of collide, if Europe does decide to try and force Google.com to delist, that then becomes extraterritorial to the U.S. of the EU privacy right, because then when we, Google, a Spanish lawyer, we won't get that foreclosure notice either. Although I actually spent some time puzzling on my endless airplanes, to get here on whether a Google search result is commercial speech, is it expressive speech, is it speech at all? I think it's probably best commercial speech. It's certainly in the copyright area. A lot of what they do is considered speech of one kind or another. But it wouldn't be some First Amendment issues with enforcing those kinds of directives here.

PROFESSOR MOCK: Shifting a little bit, one aspect of privacy is certainly not having people know everything there is to know about you. Once upon a time that could be accomplished just by moving to a different village and so the concept of a global village means you can't get there, you can't get out.

Another aspect of privacy is the right not to be pestered, and that goes to marketing and spam. I know the Canadians have recently enacted anti-spam law which is rather interesting. Alison, would you care to tell us a little bit about that?

MS. HARKINS: Sure. Creating an anti-spam law, CASL is what they called it, it is an opt-in regime, and the interesting thing is, it's got huge penalties and it applies to individuals, as well as to corporations. So an individual sending individual e-mails that would be deemed what they call commercial electronic messages would fall under CASL. Even LinkedIn messages, certain social media might be considered under that -- under CASL. The more intriguing thing, it's going to have a private right of action.

So if individuals feel that they are being pestered, then they will have a private right of action under CASL to bring a cause of action. In most countries, including the United States, there is no private right of action. So this is -- it's very modern. Like I said, it discusses social media, because it's one of the newest. A recent company, and, again, I don't know much about them, it's called Compufinder, but they were recently fined for four months' worth of violation sending unconsented spam and also having opt-out links that didn't work, $1.1 million. So it is significant. The penalties can be $10 million for corporations and up to a million dollars for individuals. So it's something to definitely pay attention to and it's -- it will be interesting to see how -- there are certain exceptions. There is this kind of preexisting business exception concept. It goes back two years, and you can't go -- you can't send stuff to, say, a prior client that you had ten years ago, but there is some exceptions to it. But it's certainly not carte blanche, and definitely there are ways to -- most counsel are advising people to -- if you're dealing with folks in Canada, to get a refresh of your consent in those areas.

So existing clients, try to get a refresh so that you can move forward and make sure that you're safe in that area.

PROFESSOR MOCK: Is there any sign that that will be significantly more effective than, for example, the federal Do Not Call List, which I had the pleasure of telling callers about at least two a day?

MS. CHATILLON: Don't get me started.

(Laughter.)

MS. HARKINS: Well, I think it will be interesting. I think the penalties are higher, so maybe it will be. Part of the reason that it came about, which I think is really interesting. The FBI were here and they were talking about these clicking on links and how that's really bad and how these phishing malware. That's really why Canada enacted this.

They enacted it because they were having a lot of problems with this -- so, yes, it is some anti-pestering but it actually goes to a broader thing, which is a lot of this spam contains malware and other things. That's really what they were really aimed at. So it was those things, and that's why the penalties were so big in the area.

But it will be interesting to see, but they do seem from all actions that they are very eager to start enforcing it, and it will be enforcing it and the penalties will be substantial.

MR. FRIEDLANDER: A lot of those e-mails with phish, the spear phishing come from overseas. Does the Canadian government have any plans to –

MS. HARKINS: That's a great question. It's a great question. But, I have no idea. There's no way that they would be able to limit that. But I think that that is their purpose in putting this together. Whether they will have any effect on reducing that for their citizens, I have no idea. That's pretty new so –

MS. CHATILLON: Do they have class actions in Canada?

MS. HARKINS: They do have class actions in Canada.

MR. FRIEDLANDER: They're catching up with us.

MS. HARKINS: And for the statutes, they had class actions. Class actions are permissible.

PROFESSOR MOCK: And will this new law apply to U.S. marketers reaching into Canada?

MS. HARKINS: That's correct. Anybody -- anybody, including any employees who are located within Canada. So if you have a U.S. company but then have Canadian employees, it will apply to them.

PROFESSOR MOCK: Well, it's interesting, because, if I recall, a lot of international law is based upon an argument from the 1820s in England, that you should have international law rather that conflict of laws that approach internationally, because the court of Trinidad and Tobago should not rule the world. I think that was the phrase.

That so, aren't we facing the possibility between the Canadian and the anti-spam law, CASL, and the European privacy directive and the American opt-out approach, that we're going to have so many different approaches to the same problems around the world? And we're essentially dealing with a global problem; we are going to have a great deal of

conflict in terms of how we actually enforce these.

MS. CHATILLON: Yes is the brief answer. I think one of the -- certainly from the perspective of counseling start-ups in New York in eCommerce and on the business, they all want to sell in Canada, certainly any -- I have one client who's an e-Book distributor. And most books are in English, so any major English language market is something they're interested in. Certainly Canada and certainly England. But one of the things when you start talking to them, aside from the tax and the registered to do business, that and all the other stuff is, you have to set up the way you collect and process data, the way you market, to take into account the different laws of these countries and especially for small companies that have only have $X spend or they can't pay their rent anymore, and your hoping to get revenue in before then. Setting up a database to be able to, A, get the kind of notice they need to record it in a way they need to and to delete the data in a way that U.S., largely California being always the exception to this, does not require, is one of the things they kind of look at and go, ah, I can't do that, to which the lawyer's answer is, then you shouldn't be doing business in Europe.

MR. FRIEDLANDER: It's a big problem for multi-nationals, especially since a lot of multi-nationals like to try and consolidate operations for efficiency, for cost savings. and trying to counsel clients with respect to requirements of other countries, and what data you can bring over, what it takes to bring over, what you can do with it, what happens if, for example, even an employee -- a lot of employees you have to get their consent to bring their data over. What happens if they revoke that consent? It's -- it's a big implementation problem.

MS. CHATILLON: Gary, may I ask a question?

MR. FRIEDLANDER: Please.

MS. CHATILLON: What is, in looking at the EU privacy directive and its moving into a regulation from directive, is the different interpretations of the different countries and whether multi-national corporations are looking to locate their servers in countries that have in more amenable interpretation of the directive/regulation, is that a factor people are starting to take into account.

I know certainly Google and Apple and Facebook are all building service in Europe and –

MR. FRIEDLANDER: Right. Yeah, I don't know if all multinationals are doing that. I know a lot of the laws that are coming out as

derivatives of the EU laws are requiring some sort of localization of servers, which is a bit of a problem form multi-nationals with respect to efficiencies and processing because their local affiliates may not have the resources or capabilities to do certain processing and so they want to do cross border transfers, and a lot of these laws aren't taking that into consideration.

Ultimately I think those -- I think those laws are going to have a negative fiscal impact on the countries that are implementing them, because they are going to make business so much more difficult to do, and it's going to require a greater investment.

So like a Google, Facebook, yeah, maybe they can afford it. You get a much smaller company that wants to branch out internationally, even with innovative technology, they are going to have a hard time -- they're going to have a hard time doing business.

PROFESSOR MOCK: Your last comment suggested that there are companies that are focusing on the physical attributes of their information systems where it will locate the servers, physical items, and yet we're talking much of the information is out there in some sort of virtual settings in the cloud or -- are we perhaps going by regulating this the wrong way?

Every place is -- we're trying to stick to our territorial answers, and yet we've got something that really is not territorially based. It's almost an accident where the server is or which information is on which server.

MR. FRIEDLANDER: I think you're actually correct. I think we are going about it the wrong way future-looking, because more and more will go in the cloud. It really doesn't matter where the equipment is located at, but I think a lot of countries, and I work with a lot of emerging nations, and a lot of them are, as part of their privacy regimes and other regulatory regimes are requiring things to be done in country; localized servers, localized -- completely localized businesses, localized services, thinking that's a way of creating jobs. I think ultimately -- like I said, I think ultimately it's going to do more harm than good, but I do agree, I think a lot of nations are looking at it very territorially, and maybe -- maybe when the next generation assumes power, maybe that will change because a lot of them are used to being under SmartPhones and their data is going everywhere.

MS. CHATILLON: And isn't some of that also a reaction to the NSA revelation to Snowden?

MR. FRIEDLANDER: Big part of it.

MS. CHATILLON: Yeah, because the position that our government

has taken, as I understand it, having access to nothing other than lawyering papers, that any data that comes through the United States, and most data, unless you really spend time not doing it, does -- so much of the work capacity is here, is something that the NSA feels free, or whichever agency it feels is legally authorized to do so, will tap into and many other people in the world, including some U.S. citizens, object to that.

MR. FRIEDLANDER: Yeah, I mean, the NSA revelations certainly put a giant spotlight –

MS. CHATILLON: Right.

MR. FRIEDLANDER: -- on not just what our government is doing, but what a lot of governments do, but it also showed what the true nature of the Internet is.

The Internet is global in nature. You can send an e-mail from yourself to a colleague in this building, and it could wind up going through servers on the other side of the world before it comes back here, and I don't think a lot of governments understand that if they're enacting these laws.

PROFESSOR MOCK: I usually make the claim that it has gone to other countries and now it is incoherent upon receipt.

(Laughter.)

MR. FRIEDLANDER: I'll have to use that.

MS. HARKINS: I think that some of the countries that are most concerned about this, like Russia, China, some of these are countries that they have -- they have big concerns about the United States' access to their information. China wants to obtain -- they're trying to enact things where they obtain source code and other information so that they can obtain that kind of information from -- from commercial entities that we're doing business there. So that would be kind of an interesting twist.

So, obviously Russia still has -- the localization law, I think it goes into effect in September of this year? So that will be interesting to see how it -- how it plays out, because right now it really -- people are just sort of kind of just gearing up for it, you know. How will that play out for Russia? Will that reduce commerce there?

MS. CHATILLON: That's a law that requires anyone doing business in Russia to have the capacity to confine their data to territories in

Russia, and some people think it's so that Russia can shut down the Internet if they want to and still have the capacity to process data.

PROFESSOR MOCK: Well, the Internet, after all, is kind of a pipeline.

MS. CHATILLON: Absolutely.

PROFESSOR MOCK: This discussion about moving into China and Russia at this point reminds me that following -- well, following World War II, a lot of the world's antitrust laws and banking laws and security laws were based upon the U.S. models. More recently when we had other areas of commercial law coming up for example, sometimes the European laws get in, do you see the European model, the Canadian model, the American model? What models do you see going out to the rest of the world as the models to be developed upon in the next five, ten, years?

MR. FRIEDLANDER: I think -- I think there are two different models that we're going to be seeing coming into effect it's not the U.S. model. It's going to be -- from what I'm seeing with respect to new laws coming about, it's the EU model, then there's also an offshoot in Asia Pacific.

So the APECT, Asia Pacific Economic Cooperation Treaty, they're working together for regional framework, which helps allow cross-border transfers and builds up the economy in that region of the world.

I think -- I think that's a superior model. I think from an economic perspective, I think that's going to help APECT. I think it is helping APECT. I think we're seeing a lot of the economic growth now come out of Asia Pacific, now more so than anywhere else in the globe.

It might be something that eventually South America might do, if they ever come to their senses. Right now they're all grasping on the EU model. In fact, there's one country that I can't remember which it was, but they literally took the EU directive, grammatical errors and all, and just plopped it into a law. So I think those are the two models we are going to see. It's definite not going to be the U.S. model.

MS. HARKINS: I think almost all other countries', either model, is going to require -- most countries require some sort of data transfer agreement in order to go out to a lot of other -- to countries that they deem, "inadequate" and like the EU deems most countries, including the United States, inadequate. That's the word that they use from a data protection standpoint.

So there are various methods you can use to obtain, to transfer data out of the EU model.

But I think what you'll see in a lot of these other jurisdictions, say,

countries like Australia, is you are going to have -- they are going to require some sort of data transfer agreement as well.

These data transfer agreements are, generally speaking, going to have some basic requirements, here's what's going to happen, but also, probably some security requirements as well. So that's -- they want some comfort that data of their citizens is being protected as it's going around the world into other countries.

PROFESSOR MOCK: Okay. At this point, I have no more questions, but, first of all, I want to make sure we had some time for those of you out here who have questions.

Yes. Please tell us your name, and then I'll repeat your question.

FROM THE FLOOR: My name is Greg Apollo. Given the current environments between the U.S. and the EU and with the, as you mentioned, Snowden revelations and the new EU privacy directive being replaced by an actual piece of legislation, what are your thoughts on the long-term viability of the Safe Harbor program?

PROFESSOR MOCK: The question was essentially: what is the long-term viability of the Safe Harbor program.

MS. HARKINS: I think it's going to be interesting. There are certain countries, for example Germany, that really do not like Safe Harbor and, in fact, often do not honor Safe Harbor. So, in other words, they insist on model clauses or some other form of commitment.

It's not enough to say, I'm Safe Harbor registered and whatever in Germany. Now, there are other indications, such as a working party, European working party, that are coming up with some suggestions on how it can be improved. So there are certainly some indications that they're willing to try to keep their regime with, perhaps, some improvement. So it will be interesting to see.

Thus far, it's still viable. There's no indication that it is completely going to go away tomorrow, but there's definitely some talk and rumblings in the community.

FROM THE FLOOR: My name is Matt Heary. You guys touched on the Russian localization law a little bit, and I was just wondering from a practical perspective, how you're seeing or how you're recommending companies handle that change, whether you're expecting people to just sort of put their Russian data in Russia and cut it off despite there being some allowance for international transfers? Or if there's some other mechanism you're seeing, sort of how we understood it is the way to try to comply with that change.

PROFESSOR MOCK: The question is essentially: how would you recommend clients deal with the Russian localization law?

MR. FRIEDLANDER: So you, obviously, have to comply with it. So you are going to have to put all of your data in Russia if you're going to want to do business there. I also think you need to think long and hard about what your -- what your future plans are in Russia at this point.

It would, could, end with this. It could get worse. It's clear Russia wants to seal themselves up a little bit right now.

We are seeing some companies leave Russia right now. I believe Visa and Master Card are having a bit of a difficult time.

Russia has threatened to actually create their own card payment system. Whether that's feasible or not, I really don't know. It could just be a bluff. But I believe there are some provisions for some cross-border transfers, but I believe it requires some kind of approvals to do that.

FROM THE FLOOR: There is still the consent piece, so if you collect data at that point, the user or the individual consents to the data transfer. That part, I believe, anyway was preserved in the law. But the localization piece, I think it has to be in Russia first and then it can be transferred.

MR. FRIEDLANDER: That's correct. The servers need to be in Russia and the data needs to be in Russia, yes.

PROFESSOR MOCK: Other questions?

Okay. While you're thinking, I am going to follow up.

As I listened to the description about localization laws and about some of the laws that require that you satisfy the local version of the privacy laws, I am reminded that post-World War II with a lot of countries coming into the world system, there were a larger number of import substitution laws. There were a large number of laws that were local content requirements. It seems to me, and I'm wondering whether this is accurate, that there is a parallel history in the international trade and goods, which tried to obtain local control through a variety of such laws. And now we're going through the same process with the international control of the Internet.

Any thoughts on that? Now, mind you, I admit that that's a professor's question to begin the discussion. Are we looking at the idea that we're going to go through a period of basically national warfare over these laws followed by some sort of system whereby it's all going to have to become harmonized if we're to continue forward?

MS. CHATILLON: I'll take a stab at that. I think what we we're looking at -- I would consider it a Bulgaria, the part of the EU that's a little bit more of a regional, the sort of the North America. Canada has

a view, but they're not that far from where we are. Europe has a view. South America is still struggling, I think piecemeal. I don't know -- the core issue that none of us have solved, because we're too cranky a species, I think, to come to some kind of agreement on this, is that the Internet is international. It is always international, except perhaps for China, North Korea or some other places. It takes extraordinary efforts to cut off their citizens.

If I'm posting my blog from my office on West 14th Street in New York, you can get that in Abu Dhabi and Sri Lanka and all sorts of places that my parents still barely know where they are. How do you make me conform to the Sri Lankan laws if I happen to be writing about somebody who's within their borders or their concerns?

I don't know that we're ever going to solve that problem, and I think one of the scarier and more interesting is, are we then going to cut off from the rest of world because we don't like the fact that we can't solve for that.

MR. FRIEDLANDER: I am just going to throw this out. This has sort of dawned on me. One of the issues has been, can the governing body, and I don't know what they're doing half the time, other than coming up with new domain names and charging a lot of money for it. But I think there is a historical precedence for this, so I think it's called the World Telecommunications Union that meets every couple of years and harmonizes the laws with respect to -- with respect to telecommunications, radio frequencies, this and that. Maybe that's the model we need to look at with respect to the Internet. Maybe that's not the body to do it, but maybe, ultimately, that's the model with respect to something very similar to radio waves, something global in nature.

PROFESSOR MOCK: So perhaps we have to develop a harmonized system of some sort, perhaps through eBay, perhaps something negotiated on each level.

MR. FRIEDLANDER: Yes.

PROFESSOR MOCK: And how do you counsel a client in that sort of climate when you talk about the across-the-border challenges and will be seen in Abu Dhabi or read in Abu Dhabi. Of course, you will. We have some problems in the international arena directly coming out of that example, the challenge of micro tourism.

MS. CHATILLON: Yes.

PROFESSOR MOCK: England has very easy laws under which to allege libel.

MS. CHATILLON: We had a revolution to avoid their laws, literally, as I said, in courts in London and Canada in the past, and in that, there are two things that have happened. One, U.S. passed some statutes saying you can't enforce your own constitutional libel laws here, goddamn it, and London, which became unseemly for the lords in the High Courts of Justice, that all these Russian oligarchs were coming into London and suing the Wall Street Journal and Vanity Fair, literally.

So England moved away from the one copy here gives me jurisdiction no matter what else is going on, and that's calmed down a lot. That is a continuing problem. Certainly, and I think it's practical advice, if you're writing -- if you're a content publisher and you're writing about something in another country, you either take the risk blind or you inform yourself or your lawyers about what the local applicable laws are and decide whether or not you want to publish there.

If you want to take orders from book readers in the UK, then you better comply with their tax and their data privacy laws and their credit card laws and anything else that applies. If you decide not to, then there are consequences to that. I don't know any other way around it.

MR. FRIEDLANDER: I think that's right. It's an education process that the world is not the United States.

MS. CHATILLON: At New York, we covered.

MR. FRIEDLANDER: It sounds stupid, but it's true. I mean, we tend to be very U.S. centric here and businesses tend to be U.S. centric, and I think it is an educational process, that if you are going to do business and it's going to affect something overseas, you need to be aware of those laws. So you're right on.

MS. HARKINS: I think that this -- when we're looking at projects and it crosses borders -- I'm working with a company that -- I mean, we look at all of the different laws and we look at all that are going to be impacted, all the different jurisdictions, and all the laws and then we make some judgment calls. I mean, there's, -- even as simple as having opt-out footer that satisfies all the countries' laws, for example, that's hard to do. Each one has -- well, you got to add this and then you have to add that sourcing, then you got to this, and whatever else.

MS. CHATILLON: Placed above, placed below, to the side.

MS. HARKINS: So it's very interesting, and at some point you just have to say, you know what, this is pretty darn good and it covers the majority.

MS. CHATILLON: Good enough.

MS. HARKINS: It becomes good enough. And it's probably not going to be litigated over this one little piece that's missing and so that becomes an element.

MS. CHATILLON: And I think that's a big part, certainly, of what all of us do in actual practice, which is you do realistic risk assessment. If I'm doing business and I'm going to get ten orders a year out of this, as opposed to 100,000 in it somewhere else, I pay attention to the 100,000. It is probably not going to get me in trouble. And sometimes it will and you can get in trouble.

PROFESSOR MOCK: Please, sir.

FROM THE FLOOR: Speaking of libel laws –

PROFESSOR MOCK: Who are you, sir?

FROM THE FLOOR: I'm Dan Rasolo.

PROFESSOR MOCK: Thank you.

FROM THE FLOOR: Do you see any movement away from the way we got the system where Internet providers are not essentially libel for libel or slander that shows up on their websites? They're not libel –

MS. CHATILLON: If it's third-party generated, yes.

FROM THE FLOOR: At the same time, that seems to be that there is some -- that's kind of getting chiseled away in some of state case law. But am I right in thinking that way or is that –

PROFESSOR MOCK: The question is about the evolution of libel laws under the pressures of the international.

MS. CHATILLON: For a brief bit of background, there is a statute, one of the few passed in the Internet era by Congress, Telecommunications Decency Act, which for these purposes have little to do with decency, which essentially say that if you're an Internet service provider, you're not responsible for torts committed by third parties posting on your site, passed in the '90s to allow the Internet to bloom.

I don't think it has been chiseled away. There have been a few cases, like the Dirty, which is a famous case, I think out of Illinois, that

this was revenge porn, or revenge site, and the judges were terribly offended and really wanted to hold the website libel. But it was reversed on appeal, so I think no.

I don't know if there will be a movement, again, given revenge porn and some of the really outrageous misbehavior damaging. I think we can all agree behavior on the Internet and domestic, it is not -- these are not pirates coming out of obscure atolls somewhere in the Pacific.

Whether there'll be some movement to amend for really malicious stuff or something like that or to allow the states to step in. It wouldn't shock me as a matter of policy, but I don't know of any proposed statutes.

MR. FRIEDLANDER: But that only applies directly as a conduit, more or less, right?

MS. CHATILLON: It applies to Facebook. Most of Facebook is covered by it, because most of Facebook is not Facebook-generated content. It applies to a certain amount of Google. It applies to big social media sites. It applies to the comments of the section. It doesn't apply to the Chicago Tribune site and the stuff generated by the Chicago Tribune or ABC or CNN or NBC or New York Times. They're still as responsible on the Internet for what they digitally publish as they are for what they publish in print.

But unlike in print, if I print the letters to the editor and it says something nasty about Professor Mock I have to defend, I, as a publisher of a newspaper am responsible for that, even though it's a letter from a reader and that rule does not apply on the Internet in the U.S. as it currently stands.

PROFESSOR MOCK: As I recall in the legislative history for that, it involved arguments that well, we just put up a wall. You're the ones who put up the posters, something of that sort. How could the wall become liable?

FROM THE FLOOR: I was thinking about some of the Topix cases, and I haven't been following this as closely. I don't know if you've seen those or are familiar with them. Topix is a website that essentially is your town gossip website. I think it's T-o-p-i-x. And when you get in there, there have been these cases where, first of all, they have been forced -- they were one of the first ones to be forced to start to turn over the names of people who are provided content. I know they got hit a couple times for the content. The stuff people put there is horrendous, just awful.

MS. CHATILLON: And there is also no -- unlike the DMCA where

there is a takedown, even though the website that complied with the Safe Harbor provisions is not libel for copyright violations committed again by users of third parties who post. There is a takedown regime under the DMCA, as ineffective as it sometimes is, and there is no such takedown under the Communications Decency Act, which means, even though you're yelling and screaming that this is libelous and ruining your life, the website has no obligation to take it down. Again, I think that's certainly something that people would -- a lot of people would agree should be looked at again. I don't know of any current move to do so.

MS. HARKINS: I think there's a few statutes out there that are important or kind of -- I'm not sure how detailed they are and at what level they would go to as far as -- and what would be the recourse. But there are a few in California.

MS. CHATILLON: California. You got to start in California.

MS. HARKINS: It always starts with California.

MS. CHATILLON: A separate country.

MS. HARKINS: There are five or six other states that are currently considering it. I'm not sure if any of them have passed. I believe California's might have passed. But the rest of them no, but, again I don't know if it would -- how far that those rights would extend.

PROFESSOR MOCK: At this point I note our time is up. I want to thank the audience for its wonderful questions and for being here and encouraging us on. I particularly want to thank the members of the panel. Please join me.

(Applause.)

PROFESSOR SORKIN: You know, there are also some interesting cases on rip-off report on some of these same issues for more research, as I prepare for my courses this summer.