UIC John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 4 Article 10

Spring 2015

Legal Problems in Data Management: Ethics of Big Data Analytics and the Importance of Disclosure, 31 J. Marshall J. Info. Tech. & Privacy L. 641 (2015)

SESSION EIGHT:

ETHICS OF BIG DATA ANALYTICS AND THE IMPORTANCE OF DISCLOSURE

MODERATOR:

DAVID SORKIN
PROFESSOR, THE JOHN MARSHALL LAW SCHOOL

PANELISTS:

JIM LAI
PRIVACY OFFICER, HERE, A NOKIA COMPANY
ADJUNCT PROFESSOR, THE JOHN MARSHALL LAW SCHOOL

MANUEL CUEVAS-TRISAN
VICE PRESIDENT, COUNSEL AND CHAIR OF GLOBAL PRIVACY AND INFORMATION SECURITY COMMITTEE, MOTOROLA SOLUTIONS, INC.
ADJUNCT PROFESSOR, THE JOHN MARSHALL LAW SCHOOL

PROFESSOR SORKIN: Our final speakers will address the Ethics of Big Data Analytics. I would like to introduce Jim Lai and Manuel Cuevas-Trisan. Jim is with HERE, a Nokia company, and is an adjunct professor here. Manuel is with Motorola and is also an adjunct professor here.

MR. MANUEL CUEVAS-TRISAN: I guess we have the enviable task of being the last in line. Hopefully, we will keep you interested.

MR. JIM LAI: So we have apparently entered the cloud since this is loading on PowerPoint online, so we'll see if this works.

My name is Jim. I work for HERE, which is a division of Nokia that focuses on location analytics and primarily in the areas of mapping and connective fields. So I am going to cover what big data is in terms of how it affects you and I in our everyday lives. I am going to look briefly at what are the benefits and costs of moving towards a big data environment. I am going to raise some questions about -- that we should all be asking our clients in terms of how we can identify and manage the risks that are unique to our particular implementations of the data, and then Manuel is going to answer them. I have the easy part, I guess.

So one thing I want to start with is that this has been going on for a very, very long time. One of first documented use of predictive analytics actually dates back to the 17th Century when proto public health experts mapped out cholera outbreaks and figured out that tainted water supplies were responsible for spreading this disease. So they were able to implement steps to make sure people had clean water, and lo and behold, the outbreaks stopped. So this is not something -- the concept of doing this isn't something that's really new. What is new is the volume.

Our keynote speakers were talking about gigabytes and terabytes. The numbers get very much larger than that. A couple years ago, the total volume of data, it was just astronomical in scale. I mean, normally these are numbers that only astrophysicists actually talk about.

Modern big data talks about sort of four key distinguishing characteristics that separate it from more traditional analytics. We talk about its volume. Big data tends ingest information from a variety of different sources that may seem unrelated, and they don't necessarily care how correct it is. Principally this is due to the effect of the wisdom of the crowds. So if I have a lot of data, the likelihood that most of it will be accurate is enough for me to identify some useful correlations -- it's going to be true, and if there's some mistakes, they're pretty much going to get drowned out. Then the last characteristic is that this analysis is happening very, very quickly, and it's happening in almost real-time.

As data is being ingested, the analytics are running and the models are -- and the results that are being produced can be consumed very, very quickly. There's a fifth V that I want to talk about, which is value and why people care about this.

Companies are figuring out that it doesn't necessarily matter what the data is, and I don't necessarily have to have a specific need for that particular element right now to be able to generate value. So as a result, there's only money in this business. Google, which has had Google Maps for years, recently bought another mapping -- GPS company called Waves for $900 million. Amazon bought a company called Twitch TV that let you watch other people play video games for over a billion dollars. Then Facebook has probably done one of the biggest acquisitions in a while. It spent almost $20 billion to buy WhatsApp, which was -- essentially if you don't live in the United States, that's what you use to send instant messages to people.

So you have to ask yourselves, keep this in the back of your mind. Why are these companies so valuable? What are the kinds of things that, in taking this data into their analytic environment, can do in order to generate benefit for the company? The more you let your brain spin on that, I think the more interesting things you're going to come up with.

Really what it boils down to is being able to determine likely truths that may become useful to you. A few years ago, Google made a lot of news when they released their flu trends project where they correlated certain kind of search results and were able to fairly accurately model flu outbreaks in the United States.

That being said, this project also reveals one of the weakness of big data and that sometimes your models can go bad. While the data was very accurate a few years ago, it's no longer accurate anymore, basically due to the changes in the way people actually search Google and the way that they generate data. So one of the things that we need to consider, if we're looking at big data business, is how sustainable your algorithms and your models are going to be, and it can make people uncomfortable.

One of previous speakers beat me to the punch on Target. Apparently new parents are more likely to purchase a few different things. Another company in the UK, if you're familiar with a grocery chain called Tesco, figured out that people who buy diapers and baby formula also tend to buy beer, apparently because dad isn't going out to the bars. So if you are a Tesco loyalty program and your purchasing respect habits indicated that you were likely to become a new parent, you would get ads for beer and you'd get discounts on your favorite brew, because they figured that you were more likely to buy it, similar to the Pop-Tart theory that we talked about earlier.

This is all when the algorithms are right. Sometimes they screw things up, though, and it meets instances where big data can actually cause real harm that is -- that's more tangible than something just making me feel uncomfortable.

Calwin was a, and I think it still is, a medical -- a state medical benefits administration system. They implemented some data analytics, and as a result of some errors in its assumptions, Calwin automatically terminated the benefits a large number of people in the state. So people would try to get health care and it turns out that their insurance had been cancelled, and no one really knew why, because no one really understood what the algorithm was doing, so this caused a big problem.

Then, finally, related to getting things wrong, it can create assumptions about us that we -- that may not be transparent to us at all. On the left here, there is a screenshot of an Amazon's product recommendations page. What the product -- what the searches for was for a digital scale. It says the customers who bought digital scales also tended to buy resealable plastic bags, filter tips, rolling papers, and you scroll down the list, you also get fire -- you also get safes. So these are all based on -- these are all based on real correlations, but the way that they are applied to human beings can have an impact on our lives.

LaTanya Sweeney, she's an academic who decided she was going to Google herself. Apparently at some point Google's algorithms took her name and made some assumptions about her. These -- and the panel on the right was an example of some of the things that it was recommending that she click on, even though these were completely relevant to her actual life.

And then, you know, finally, as a result of all these, people can be subject to discrimination that they may not actually know about.

Orbits is a travel website. You can buy flights, you can reserve hotels, do all kinds of stuff. Everyone who has a computer or mobile device has identifiers associated with that machine that tell any website you visit something about the machine itself. So it's maybe the model, the make, what version of the software you're using, a couple other basic statistics that wouldn't ordinarily seem particularly descriptive, but apparently Orbits figured out that people who buy Apple products tend to spend more or make more money than people who use Windows products. So they tailored their search results based on what kind of computer you had.

Other similar correlations that have been in the news recently, have covered things like a certain kind of people who buy certain kinds of SmartPhones are correlated to having a have higher IQ than people who buy other kinds of SmartPhones. When these sources of algorithms are used to generate results that we see and provide us with choices that -- the choices that we get to pick from, they may not actually be based on reality, but, rather, instead on the sort of invisible kind of data profile that has a lot of correlation -- that has a lot of correlations but may not necessarily apply to us in our particular instance.

Then, one of the things that privacy folks talk about a lot when it comes down to managing these large data sets is this notion of anonymization or deidentification. You take information about me, so you may have my name, my e-mail address, maybe the serial number of my phone, you strip out a lot of that information and kind of drop it into a large data set with a bunch of information from a lot of other people.

And the goal of anonymization is to make it harder to identify an individual within that data set. In the '90s, in the early days of the web, there was this cartoon. It's the cartoon on the left with the dogs, and there's a recurring -- there's an ongoing effort to determine when deidentification is good and when it's bad. If your deidentification techniques are not good, then it can become a lot easier to pick a single individual out of that data set and figure out who they are.

One of the more recent -- one of the more recent examples of this, was it took the locations and times of credit card purchases in an anonymous data set and we were able to figure out which individuals were associated with which cards. Ultimately, the cause for that is that they didn't really do their deidentification very well, and so if you look at the HHS guidelines, for example, for HIPAA electronic health information, there are 18 different kinds of data elements that should be removed from any kind of data set for it to not count as PHI under HIPAA, protected health information.

So getting anonymous -- getting your deidentification wrong is pretty much a sure way not -- to have it not work due to the volumes of data that are being ingested and the speed in which you can run operations on that information.

And so as practitioners, there are a few questions that we want -- that we need to ask people, our clients, when we're evaluating their data privacy. Some of these are privacy related, but not -- they take into account a lot of other interests, as well. One of these is who are the stakeholders who have interest in this information? That can be your client, but that's the individuals who sort of provided the data. It could be -- it could be your client's customers who are relying on your clients to analyze that data and generate useful information for them.

But we need to figure out who those stakeholders are so we can figure out how doing this big data project is supposed to benefit or harm each of the -- each of those stakeholders. Ideally you want it to be a positive sum experience where everyone derives some kind of tangible benefit out of this project. If what you're analysis finds is that that not be the case, that some people may -- that there is a risk of harm to some of these individuals, maybe that should make you think about what mitigations can we put in place? What can we do to control for those harms and move us further along towards that positive sum experience? Then, finally I want to go back to the Google food trends, and keep in mind that just because something works today doesn't mean it's going to work forever.

So it's really important for us as practitioners to understand how sustainable is this project going to be, how long lasting is this model? The answers to that are going to inform a lot of things, including topics we've already covered today, including retention, when to anonymize data, how long to keep selling the results.

So if you think about questions like that, you'll be able to generate the kinds of useful counsel that I think a lot of technologists don't really understand, because they're focused -- they're more focused on the numbers and not necessarily on the unintended consequences of what we're doing.

I think Manuel is going to answer all these questions for us and so we will never have to do any hard work ever again.

MR. CUEVAS-TRISAN: Thank you. All right. Then we will come back to Jim after I finish my part of the presentation. But it's a great setup for what I'm going to be discussing, and what I'd like to do is to try to bring to light some of these questions that -- certainly ethical issues of what kind of principles we should adopt in dealing with big data in a real life context. In the case of the company that I represent, Motorola Solutions, which is a Chicago-based company -- or Schaumburg-based, but really a Chicago-based company -- I am trying to bring to life the issue by discussing big data in the context of smart policing.

Before I speak specifically about smart policing, I would like to say a couple of things. There has been a lot said already about big data, about what it is, what it is not, but there's one thing that I haven't heard during the course of the various presentations, which is that the reasons why there is a significant value, and there's a whole economic underlying concern relative to big data, and a lot of the discourse and the EU, about the right to be forgotten and here about having more liberal rules about managing data, is that the cost of storing data has been steadily reduced. It's cheaper and cheaper to store data these days, and we saw some examples of that, so much so, that it's becoming cheaper than actually destroy it. So destroying data and disposing of data is now more difficult, more cumbersome and more expensive than actually storing the data. That is a key item to consider.

Number two, when we talk about big data, we cannot just think of big data in terms of the Internet of things, but very, very complete applications within the workplace. I'm an employment lawyer originally and by trade -- most of my career has been focused on employment law -

- they are significant big data applications that can be applied in the workplace for hotel and management, looking for promotional opportunities, determining leadership potential. Those are decisions that if -- when you apply big data and you apply algorithms to the information that you have on your employees, it can lead to potentially discriminatory assumptions and, therefore, discrimination in the workplace.

But let's go back to again this particular context that I wanted to focus, and when we talk about smart policing or intelligence-based policing, it's something that is not entirely new, but it's now, because of the capability, the analytical capability, and you were talking Jim about the four Vs. In the context of smart policing, there are two Vs that come to mind volume and certainly velocity and ability to process vast amounts or vast volume of data in a very compressed amount of time.

You think about a 911 call. Do you happen to know if we can get some guesses in the audience. The average response time from the time there's a 911 call up to the point where the first responder arrives on the scene? Minutes? Hours? What would be your guess in Chicago? Anybody know?

FROM THE FLOOR: 15 minutes.

MR. CUEVAS-TRISAN: 15 minutes? So the answer is, like a good lawyer, they would tell you, it depends on the city, it depends on the neighborhood. There are a lot of variables, but in Chicago you can say that the average response time can go in some neighborhoods from 2.35 minutes to five --sometimes up to 9 minutes, but that is in relative terms. Actual terms are fairly compressed amount of time.

And yet for a company like the one I represent and some of our competitors, the gold -- the gold line for us is to harness as much information from multiple data points to be able to put the first responder in a position to have greater context awareness.

MR. LAI: So this is more than a job selling ads to people.

MR. CUEVAS-TRISAN: Definitely, more than selling ads to people. It's about selling solutions to public safety agencies. So there's always an economic -- an economic component to this. There is also a huge economic benefit for public safety agencies, because what we're talking about is -- we're talking about historical crime analysis, predictive policing, and what does that mean? It sounds like a very fancy concept, but when you think about where the state of affairs, of economic affairs is for a lot of public safety and for a lot of state, federal, and certainly for municipal governments, they are scrapping for bucks. If you think of how to most efficiently deploy your resources, crime analysis and predictive policing can be very effective for making determinations about where do I deploy, for example, police surveillance? Where do I install cameras for surveillance? The dispatch -- call dispatch management. There's a huge amount of efficiencies and savings for public safety agencies and certainly opportunities for companies like Motorola and other of its competitors to sell intelligence capabilities to these public safety agencies.

The other important element is citizen engagement capabilities. There's already products in the market, including the products that we offer that allow greater engagement between citizens in a particular city and their public safety agencies and get information about crime patterns, crime information, et cetera. We can aggregate all kinds of data to be -- to put the public safety agency in a position to effectively respond and address safety concerns in the City.

And as you think about the shifting paradigm for public safety agencies, up until very recently, the main -- the main source of information for a public safety agency was voice capability, and then the dispatcher receives a call through 911, they dispatch an agent, and the agent arrives on the scene and just reports through a walkie-talkie. Right now walkie-talkies have data capabilities. Police cars have full computer screens that have access to schematics, to maps, to location data, and to all the data that a smart system has.

Therefore, they are able to, number one, predict. That's the one, at least predict, or make correlations between different pieces of data. They can then have greater situational awareness during the actual occurrence of an incident. You may recall very recently what happened in Paris with that attack. There were feeds that were almost real-time of videos that were posted of the individuals shooting. Those -- it showed the vehicle. With the vehicle, you may have access to a license plate. With the license plate, you may have access to ownership of the vehicle. You had access to a particular intersection in the city of Paris and you saw the direction in which they left. Talk about valuable data for enforcement. It was interesting that our law enforcement agency or Sheriff referred to as breadcrumbs. I would refer to this more like little gold nuggets of information.

They call it data mining for a reason. Then, of course, you have the value of the data after the incident, where you need all of the data for investigation, case management, and eventually prosecution.

So what are the sources of data that we deal with or that public safety now has access to, and we can aggregate for the benefit of law enforcement, video, and video can be private, it can be mobile-based and it can be from surveillance cameras.

Does anybody how many surveillance cameras are in the City of Chicago? Guess?

FROM THE FLOOR: 10,000.

MR. LAI: I know we are one of most modern cities in the world.

MR. CUEVAS-TRISAN: 17,000. 17,000. That's a lot of cameras. That's a lot of video feed.

You have social media feeds, geo location, sensors, sensory information, and, for example, insurance companies certainly would benefit greatly, and will benefit greatly from sensor information. Criminal justice information systems databases and, of course, DMV and other systems, including private systems, like home alarm systems.

MR. LAI: Yeah, that thing that Progressive wants you to plug into your car, that is a big data tool.

MR. CUEVAS-TRISAN: It's a big data tool and there's arguably a lot of benefits for the consumer because they may get certain brakes or certain discounts, but at the same time it's a little big brother-ish in that it follows -- tracks the location, tracks the speed, and in the case of -- think about the sensor technology, sensor that are attached to the body. Anybody have a FitBit here, tracking your steps? So there's a lot of technology that's being developed that also tracks and monitors your heart rate. People in fire departments now are testing technology where they go can into a fire and the fire department can know whether during the stress, whether they are able to communicate or not. They will know by blood pressure and many various other indicators whether they're in distress and, therefore, call for additional help in a particular situation.

So the idea of smart policing is that it harnesses the data or that broad similarly pair of data to gain intelligence and integrate it into public safety operations. Here you have a diagram that just shows here the Motorola in the middle in the cloud that again offers the notion of citizen engagement and interactive crime reporting with, of course, crime predicted analytics with the idea that you're trying to turn disparate data into actual intelligence and putting the first responders in the likely place for a crime to occur. That raises all kinds of ethical questions, potential profiling. Think about cities like Chicago, that have, again, all kinds of arguments regarding what the situation is in the south, the southern part of the City, versus the northern suburbs, that raises all kinds of ethical questions.

But what is the value proposition from a technological and economic perspective? It helps through those correlations anticipate and respond to incidents in a more informed way which good correlations and the best information. It offers the ability to make better decisions by viewing data in analytical dashboards.

And when I talk about dashboards, we're talking about very sophisticated dashboards that now police agencies are outsourcing to companies like Motorola and various other competitors for us to -- as a managed service to offer next generation 911 services, command control centers that gather all this information from all these data sources.

Predictive capabilities that we've already discussed, but make recommendations as to where to allocate resources. Think about patrolling decisions, when to patrol, because if you know that crimes are likely to occur between 6:00 p.m. and 6:00 a.m., you are going to put more patrols in a particular area rather than having the same number of patrols at a given time in that particular place.

Of course, what to watch for to best prevent crime based on historical data. Also crime mapping allows agencies to share crime information and alerts through citizens. That's a concept of citizen engagement. Improves call writing efficiency. There are numerous studies that having conducted about particular equations that put a strain on 911 systems, and a lot of times it comes from -- it's pretty significant and involved multiple crashes and terrorist events that systems get overburdened, and with greater intelligence, including the location data, the distribution of calls can be made much more efficient.

Then, of course, citizen crime team management platforms that allow citizens to engage and provide information that then aggregated with other information can help with these predictive capabilities. But, of course, the ethical dilemma I think I am going to ask more questions than provide answers. But the reality is that, and I think somebody said before, the fact that there is going to be all that information out there doesn't mean that -- and even if it's available -- doesn't mean that we own it, and, therefore, it doesn't always mean that we can use it.

In other words, the fact that we can use it doesn't necessarily translate into an actual use. So what are the -- somebody I think coincidentally used the phrase balancing act. Nothing particularly original about that, but it is in the end a balancing act. We heard about risk management approaches in our prior panel, that as legal professionals, you are going to be or privacy professionals, you are going to be required to counsel on both private and public organizations about what to do with a particular big data solution.

The way I try to approach these issues always, and there are multiple ways to approach it, I will just offer mine, is just to do a balancing of interest test. Ultimately you want to comply, but the answers in this area are very rarely clear, and the solutions are very, very linear, as well.

So what you need to understand is what are the interests that are at stake and the typical interest that come into play under our part of the current discourse right now is the issue of privacy versus security. We talked about the importance in other panels about transparency, about providing adequate notice to individuals. Where consent is required, make sure that the concept document and that the use policies that you are going to be counseling about are clear and are in plain English Disclose the actual uses that you are going to give and if those uses change over time, you make sure that you provide a renewed notice so people understand what those uses are going to be and how those uses are intended to evolve, especially if they are foreseeable.

Number two, this concept of balancing between the social harm from a surveillance tape or a big brother in the context of private enterprise verses the benefits and the convenience falls in this category improvement of the quality of life. You get more targeted advertising. That is good, because it's more relevant, but it's bad because you may not want to be bothered with this. And that goes into your consent practices; do you go into an opt-in mode or an opt-out mode?

Number three, the balance between allocating resources efficiently versus not discriminating. And in the case of public safety, making sure that, yes, you have a database approach to the employment of resources but that in the process you do not discriminate against particular sectors of society or particular communities.

The concept of there is a value in predicting and makings those useful correlations, to use Jim's phrase, but there's a fine line between those useful correlations and actually profiling. We are going to talk -- I will turn it over to you, Jim, so we can go through the rest of the presentation. The one thing that I would say from an ethical perspective, I have always found very useful to follow a principle-based approach to privacy management, making sure that the organization that you're counseling understands what are their -- what is their philosophy, what are their principles. And among those principles, paramount always is notice and consent. You need to be transparent as to your uses. You need to be clear in explaining those uses. And you need to act in a manner that is openly consistent with those uses that have been anticipated when you design a service or a product.

I will turn it back over to you, Jim.

MR. LAI: It will take me about 30 seconds to talk about this issue of transparency and then I am going to open it up for questions. I know that there is a reception downstairs, and everyone will want to get a drink. Sometimes transparency is hard. I know I did not vote on whether to deploy 17,000 cameras on the streets of Chicago, for example. So I think this goes back -- this issue of transparency goes back to this balancing and identification of stakeholders and the design of a program --

the design of a program that is intended to be beneficial to as many people -- to as many of the stakeholders as possible so that you minimize the chance of harm. Then the way that you -- some of the ways that you can do this are in situations where you -- you can't necessarily be transparent are, for example, to deploy very strong DNA identification techniques and to have protocols in place that are tailored to your particular client in order to -- that are intended to make sure that the individuals who contributed to the correlations are not harmed by use of those correlations against them in some kind of negative way.

If you want to look at how a public facing project like this is working here in the City, I would encourage you to search for something called the Array of Things. It's a project, it's a nonprofit run here in Chicago that is deploying sensors throughout the City to create basically it a fitness monitor for the City of Chicago and the data is open source. Anyone can look. Anyone can grab it for you, academic or social, social policy and uses. The steps that they have taken to make this system as beneficial as possible for as many stakeholders in that data echo system as they have identified, it's pretty interesting read.

MR. CUEVAS-TRISAN: I have a comment in terms of how do we make a balancing act. I'll give you another example, and I know there was again reference to prior presentations to cyber security, and the issue of insider threat. Okay, so when we talk about insider threat, this big brother, not just about malicious actors within a company or an organization, but we are also talking about people that just don't follow policy, insider threat because of inadvertent failures or carelessness.

One of the things that some companies are doing are -- in fact, the federal government is going to be a requirement very soon as part of their procuring rules, that's very important for companies doing business with the federal government, they are going to require that companies have not just cyber protections and take reasonable measures to protect information, but they actually require they have an inside -- an insider threat program. And they are incredibly powerful tools that are configurable and scalable to the size of your organization and include hundreds of well-known risk indicators of insider threat.

Insider threat accounts for approximately 30 to 40 percent of all breaches. So based on the broad list of indicators that you can select, you can identify some of the most known ones are disgruntled employees, what could be the reasons to make that employee disgruntled. Unhappy with the terms of his conditions of employment, has filed a claim against the company. That's -- in the employment world, that, in and of itself, is protected activity. So we do it very, very careful.

Again, as a lawyer you -- all of you need to be -- I know you are, because we are here preaching to the choir, right? But as we interface with in-house counsel, who may not be employment lawyers that would be something to be very worried about as identifying as a risk indicator.

Other known risk indicators are, if you are in a performance improvement plan. Employees that are in performance improvement plan tend to be unhappy, if they are unhappy, they could be disgruntled, if they are disgruntled, they could be again a useful correlation.

So I have just given two examples that -- for example, nationality is an indicator, and we heard a lot of examples from our -- from our law enforcement officers, and, again, these are all real examples, and there is a -- all the examples they gave involve Chinese or most of them were Chinese nationals that were involved.

In the Motorola example, it was actually a Chinese national, as well. Being illegal absence is another indicator. Significant downloading of certain documents, so significant downloading can be another risk indicator.

So, again, as you hear the list, and there will be hundreds of these indicators, some are perfectly harmless, nondiscriminatory, and for the objected, others are particularly delicate or particularly sensitive, right?

So I'm not here to tell you or suggest that you do or you do not, but at some point where you work at or represent an organization that needs to implement an insider threat program, legal needs to be part of the equation. Legal needs to be part of that discussion to make sure that those indicators are that being configured into the predictive capability of whatever is an insider threat or likelihood of insider threat aren't -- don't run afoul of discrimination laws or privacy laws, as well.

MR. LAI: Just remember that big data is about people. None of us -- we are more than numbers, and you should keep that in your mind when you're advising your clients, that will put you in the right frame of reference.

Questions?

FROM THE FLOOR: A long time ago I used to say that whenever you write a letter, especially to a client or to an opponent, you had to write it as though a federal judge is going to look at it someday. Just thinking from this, that whenever you start searching on your computer, if something should happen to you, you have to look at it as though a policeman might look at it someday.

MR. LAI: There is a reason that Google publishes a transparency report each year. That details how many requests for user data they get from law enforcement agencies. It's a fairly big number. Your company may have a policy of deidentifying that information after a certain period of time. That is -- that is a way you can reduce that risk, because if they give me all the information you have on Jim's searches, well there may be not any left. So not only what you do with it but when you throw that information away becomes a really important consideration.

FROM THE FLOOR: You were talking about the number of cameras, and I remember the news talking about a public official committing suicide near the Chicago River, the north branch, and that public official specifically picked this spot to commit suicide where he knew there were no cameras.

FROM THE FLOOR: I just had a question on the comment that it is actually cheaper to store and maintain the data instead of destroying it. What are some of the costs that would go into destroying data.

MR. CUEVAS-TRISAN: I don't have data on actual costs, but if you think about -- there have been a number of cases reported about people having left -- I remember when Facebook -- this was about two-and-a-half, three years ago when they went to that timeline concept, our people decided to just leave Facebook, and erase their accounts. The fact is that a lot of those accounts that people erased, a lot of pictures are still showing up in other places. Remember that if you posted something publicly, in a public profile, LinkedIn, think about Facebook, people may have downloaded what you posted.

So the practical complications and inconveniences that make it extraordinarily difficult and, therefore, much -- they have already surpassed the cost of destruction, but certainly the hoops and turns and assurances that you need to obtain make it much harder than actually storing it.

MR. LAI: Getting rid of stuff is hard. What happens -- what happens when you do a refresh on your laptops, which you may have leased from someone? How do you know what's going to happen to those hard drives or your smart phones, things that you cycle through a lot?

Really, we heard from the FBI, really erasing information is actually pretty complicated. You actually -- you do more than delete. You have to essential run it through a tool that physically writes over the piece of the hard drive where those bits are stored several times in order to really destroy it. So that's a time-consuming and intensive process.

Anything else?

All right. Great. Thanks.

MR. CUEVAS-TRISAN: Thank you very much.

(Applause.)

PROFESSOR SORKIN: I would like to thank the final panel and all of our speakers today for an interesting and enlightening symposium.

Thank you to all to everyone here for joining us and sticking with us for the day. A couple of very brief announcements and then I will let you go.

First of all, as I mentioned, there's a reception immediately following this session down on the third floor. It's 3-D. So if you take the elevators at the end of the hallway down to the third floor, they'll open into that room.

If you take the stairs, you will hit a fire door and be blocked and have to come back out, so don't try the stairs.

Secondly, if you're seeking CLE credit in Illinois and you signed in when you came in, you will also need to sign out as you leave to receive credit.

Finally, there are evaluation forms at the desk in the hall. You probably received one of these on the way in, but even if you didn't, please go ahead and grab one of these forms and fill it out. We would very much welcome your opinions about the program, and also we'd like to collect some personal data from you with your consent on the back, and if you'd like to give us information so we can contact you about future programs, we encourage you include that here, as well.

Thank you all very much for coming