03062014 IAPP Global Privacy Summit Scott Charney

IAPP Global Privacy Summit 2014
Scott Charney
March 6, 2014

MODERATOR: Good morning, ladies and gentlemen. I hope you're enjoying the summit and our keynote speakers. This is the easy part for us professionals, because wait until you get into those breakout groups, so enjoy it while you can.

I'm here to introduce our next keynote speaker, Scott Charney. Scott is a Corporate Vice President for Microsoft's Trustworthy Computing Group. And in that function Scott is responsible for a range of corporate programs that influence security and privacy of Microsoft's products, services, and internal networks. Scott also manages the Engineering Excellence Team, which as the word indicates is a group that's focused on promoting the best of breed engineering practices and ensuring compliance with Microsoft's mandatory engineering policies.

Scott hasn't always been at Microsoft. Before that he was a principle at PricewaterhouseCoopers, and before that he was the chief of the computer crime and intellectual property section of the Justice Department.

Scott will be talking about an issue, a topic that couldn't be more timely, but rather than me trying to summarize it, why don't we simply ask Scott to come on stage and let's see what he has to say.

Ladies and gentlemen, Scott Charney.

(Applause.)

SCOTT CHARNEY: Good morning. It's a pleasure to be here. And I am going to talk about, as you might suspect, NSA surveillance. I travel all over the world. I talk to governments everywhere, and it is certainly the topic du jour. But it's actually not the only important topic in privacy. We are also looking at fair information practices and how it applies to the world of big data.

And the reason for this is there are a bunch of changes happening in the world that are really going to affect the way we live in dramatic ways. We have ubiquitous computing, the Internet of Things, sensors everywhere. We have natural user interfaces and voice and biometrics. We have big data in the cloud and the ability to do big data analytics. We have tailored experiences now where you want to know things about your customers so you can give them more personalized experiences. And, of course, we have data collection and use by governments.

It's very important to understand that this issue of data collection and use is really not new. A couple of years ago I wrote a paper called TWC Next. And I said there were

really three major things happening in the world that were going to reshape our strategies. One was big data. One was what we call advanced persistent threats, the idea that there are well-funded adversaries that attack networks with great sophistication over time. And the third thing was the role of governments in the Internet. It's important to appreciate how much that has changed over the years.

When I started in cyber, it was 1992, in the Clinton Administration, and they really had a laissez-faire approach to Internet development. They didn't want to regulate the Internet because it was an engine of economic growth. It was showing amazing capacity to innovate. It was an amazing protector of free speech and other kinds of freedoms and association. And so initially governments mostly kept their hands off. And like other things that have happened, then problems start to arise. In law enforcement we started getting involved.

And when I started thinking about it I realized, look, we're in the middle of our third major evolution. We were hunters and gatherers, then we were agrarian, then we were industrial, and now we're information. And if you look at the beginning of the industrial age everyone was super-excited - you're going to have cars, refrigerators, indoor plumbing, all this wonderful stuff. And people didn't think about labor strikes, unionization, minimum wage, global warming.

People go into these revolutions with all the hype, and then reality hits. The Internet was the same way. You were going to have video teleconferencing with your children anywhere in the world. You were going to have online healthcare, learning - all these wonderful things. And the cybercrime problems and these kinds of problems came afterwards. And governments over time have had an increasingly complex relationship with the Internet. It's important to appreciate that they actually have four distinct relationships.

First enterprises: governments are just large enterprises. They run really big IT systems. Their customers are citizens, but they provide services over the Internet just like companies do. They provide for e-tax filing, they want people to claim benefits online, because it's more efficient. They want you to renew your driver's license online. As a large enterprise they have to worry about their security, just like any other large enterprise.

Second, they're protectors of the Internet and the people who use it. So governments are concerned about the privacy and security of the public, and they're worried about what we call critical infrastructure protection. The idea that we've become so dependent on these systems for certain critical functions, like banking and finance, and electricity, that attacks against critical infrastructures can have grave consequence to the national economy, public safety, and national security. In that context they are a protector.

Third, they're an exploiter of the Internet. When you start thinking about governments building cyber warfare capabilities, and wanting to engage in espionage on other nation states, traditional functions, they exploit the Internet. What's different about the Internet

is when governments used to exploit each other in the Cold War there was a model that worked that didn't involve the civilian population. We put spies in their country; they put spies in our country. We'd arrest their spies; they'd arrest our spies. We'd go to Berlin; we'd trade them over a bridge. We go back and we spy again. But, the civilian population was left immune.

Now if you look at Stuxnet, which was malicious code designed to cripple the Iranian nuclear development facility, researchers found Stuxnet, variants of that malware became known. It got distributed around the world. And it exploited vulnerabilities in Windows that we then had to patch and the whole world then had to patch their systems. So it bled out of the government domain into the public domain.

And then in addition to exploiting the Internet, governments want access to data. They want it for law enforcement purposes and national security purposes. And in a post-9/11 world the government of the United States' primary mission was what? Not to let 9/11 happen again and get access to data. So suddenly we had all these data access allegations come out and it's interesting -some of the original allegations weren't true. For example, one of the first allegations that came out was governments had direct access to the servers of companies like Microsoft, Google, and Yahoo. That wasn't true. We said it wasn't true. The government admitted it wasn't true. It was never true.

Now, more recently there was an allegation that GCHQ, the government intelligence agency, was capturing video images from web cams, including nude photos. So I said to my wife, it's a good thing I've been to the gym. (Laughter.) But, governments have always wanted access to data, and we knew that because the quote I showed you was several years ago. But, something happens when theory becomes reality. When things that people suspect become verified as true it affects the way people react.

Look, the risk of four planes being hijacked and two planes hitting the World Trade Center were the same on 9/10 and 9/11. We got the Patriot Act after 9/11 not 9/10. Why? Theory became reality. But, the interesting thing about this reality is it presents us with conundrums as a society, because in this new environment in which we live, we have both governments and users of the Internet conflicted over what they want.

So for example, governments do want to protect security, they do want to protect privacy, they do want to protect public safety. And these things are in conflict. And when I talk to people, particularly those out of the IT industry, that don't think about all the nuances of encryption and other things, I've met so many people who said to me -- you know, the NSA had these big surveillance programs. I've met many people in the U.S. that have said, well, we're paying them a ton of money I hope they're protecting us. And they don't have the visceral reaction that some other people have, which is, yes, I want to be protected, but not in this way - that this kind of bulk surveillance is a problem.

And of course, Microsoft has many, many, many customers overseas. In fact, more than half of our revenue is generated overseas. It's very interesting when you think about that dynamic, because if you look at the American government's response to these disclosures

they did something that is not surprising. They said don't worry, we have constitutional protections and statutory protections, everything has been done by the book. But, Europeans don't benefit from those statutory protections, and neither do the Chinese, or the Koreans, or the Japanese. And in a global economy saying that you're protecting your sovereign borders is not a compelling answer to the globe.

And I would argue with you that basically there are kind of three thematic things that are happening where we really have not come to grips with globalization. One is on manufacturing and labor, where when you had great wage inequality, like in the U.S. in the 1900s, Theodore Roosevelt could support the unions and bust up the trusts and say we need better income equality in the United States. But, today of course labor can go offshore. You can't just regulate your domestic economy in a global economy. The power of a single nation gets diminished.

The second great example is global warming. No country can take any action independently that will significantly solve this problem. And the third example is the Internet, which is global. It is a mistake to think that sovereignty is dead. It is not. The question is how do countries apply sovereign rules in a global Internet? And how do global companies respond to these kind of challenges in the global market?

So for Microsoft actually we've had principles in place for over 10 years that have worked very well for us and as a result I have not worried about Snowden disclosures. And the reason for that is if you act in a principled way and you know what you've done, then you're in a position to say I know that my conduct is going to meet the expectations of our customers and you're in a much better position. So the three core principles that we've been focused on for a long time are security, privacy, and transparency. And I'll give you some examples of how this works in practice.

So in security we've always recognized that we have to work on defense not offense. When one country attacks another country we have one customer attacking another customer. That second customer will call us for help. And as a result of that we only do information assurance. We put no backdoors in our products.

It's interesting. Years ago I was in China and they said, we think you put backdoors in your products. I said that would be economic suicide. If we put a backdoor in our product our market cap goes from what it is to zero overnight. We can't sell anywhere in the world, including the U.S. And it was funny, because back then we had a registry key, you know Windows has registry keys for important settings, and there was actually a key called NSA Key. And the Chinese, one of the Chinese delegates said, but you have this NSA Key. And we had published about this. I said if we had a backdoor for the NSA do you think we'd name it NSA Key? He didn't bat an eye. He said that's why it's so diabolical. (Laughter.)

But, we don't put backdoors in our products. We advance the state of our security technologies. And in fact, when I got a letter from concerned citizens in Europe asking me, look, you have an antivirus product called Defender, have you ever caused Defender

not to notify a user, because it found government surveillance software? The question was easy to answer. No, we don't do that. We don't care what the source of the malware is, and we don't care what the purpose of the malware is. It's malware. The user didn't want it. It's malware; we notify.

We also have a government security program. We make our source code available to governments. Why? Governments say we can't trust your products; you have backdoors in your products. We go here's the code, right, that's part of transparency.

The second thing is, we need to support the privacy of our customers. We have never gotten a request for bulk data. If we got a request for bulk data we would fight it in the courts. We turn over account information in those countries that have jurisdiction over us when they give us as judicial order, appropriate legal process, for a specific and identified account.

Look, we have the same tension as the rest of the world. We do not like kiddy pornographers on our network. We don't want our users to be victimized. But, we also have to protect their privacy. And so we have rules in place about when we'll turn over data, and when we won't; when we'll fight the government and when we won't. And we would fight bulk requests, because we don't think that's the right way to go and we've been clear about that.

We also have transparency principles and what our goal is, is to be transparent about our activity. So we have the government security program, transparent about our source code. We publish transparency reports on the number of orders that we get from the government. We litigated with the government and it was settled when we got the right to disclose more about national security letters. And I agree with the last speaker that transparency is critically important. You have to be able to tell customers what you're doing and how you protect them and what you're willing to commit to and what you can't.

So I have some European customers who say, if you get a court order will you always notify us? I go, I can't go that far. Sometimes a court order comes with a nondisclosure order. So I will direct them to you. I will notify you if I can. But, I have to follow the law in all the jurisdictions where we do business. And then we have to advocate for the right laws.

And so having these principles in place meant when Snowden disclosures came out I really wasn't worried about the disclosures. I really wasn't. The only thing I worry about is how some of the things we've done may have been represented by others. What do I mean by that? Well, if you remember and you looked at the Snowden disclosures and the PowerPoints of interceptions of Google data centers with smiley faces, you can't control the way others represent what you have done.

So for example, we have tool called the COFEE tool. It's a forensics tool. We give it to law enforcement. You can search for it on the web. We've talked a lot about it. It's a forensics tool that when law enforcement seizes a computer and needs to get data off the

computer they can run this tool. There's no magic in this tool. If you used encryption, here I disagree with the prior speaker, if you used encryption implemented the right way it can actually be a barrier to people getting your content.

Okay. It's not risk elimination. It's risk management. With encryption people can go after the keys. People can spend a lot of time trying to decrypt, but what you want to do is manage the risk and raise the cost. So we can't break BitLocker. If you BitLocker your machine there's nothing we can do. The COFEE tool uses sets of utilities, most of which were available even before we consolidated them.

So we have this COFEE tool. So a law enforcement agent can say, hey, we seized this computer, can you help. And I can say, well, here's the COFEE tool. They can go back and write a PowerPoint that either says, bullet point, we talked to Microsoft they gave us the COFEE tool, don't tell anyone, smiley face, or they can write all they would do is give us the COFEE tool, sad face. I can't control how they represented what we've done. But, I know what we've done.

And so we have these principles and we've been very clear on where we stand on these surveillance issues. But, it's not just about surveillance, even though it's the topic of the day. We are in a world of big data. And in a world of big data we have to rethink how we apply fair information practices. And the reason for that is that if you go back to the seminal documents, whether it be the Privacy Act of 1974, or the OECD Guidelines of 1980, there were many principles about accountability, security, and the like, but principles that kind of came up to the fore were principles about collection, notice and choice.

And so in today's world the normal process is to give people notice about what data you're going to collect and how it's going to be used. And there are several problems with that. And those who want to cling to this model I think really have their heads in the sand. The first thing is that people get tons of privacy notices now. A study by Carnegie Mellon showed you would spend over a month every year just reading all the privacy notices that are put before a web user in the ordinary course of life, on the Internet. Now I'm a lawyer and I know that every privacy advocate, as well as every consumer who uses Microsoft's products, read those privacy statements, consult with their attorneys and then check the box.

But I fear that in some cases that may not be happening. And by going to notice and choice, you put this huge burden on the individual, and you allow people to put in very long notices, here's what we're doing, and look they click the box. In fact, so I am a lawyer, and I was at a website of a big media company, and I decided to read their privacy statement. So I read their privacy statement, and I could parse it. It was long, but I could do it.

And I got to the end, and it says, by the way, we share data with these companies. If you want to know what they're doing with your data, click the links. And there were a bunch of them, like seven. So I clicked the first one and I got another privacy policy. I said I

could read this until I got to the bottom, and there were seven more. And I know if I kept going, eventually they'd point me back to the first one. There's no way you can figure this out. That model doesn't work.

The other problem is that model assumes there's a relationship between the data subject and the collector of the data, but that's not true anymore. You're going to have smart thermostats in your house with no interface at all. You have GPS and Lojack in your car. There's going to be an Internet of things, and data is not always going to be collected from you. Banks have figured out that whether you're a good credit risk or not, they can look at your FICA score, sure. But it's even more interesting to look at your friends on Facebook and see if they defaulted on their mortgage. So if I'm looking at your friends and seeing if they defaulted, and then making a deterministic decision about you, what did I collect from you and what notice did you get? That model is just not working.

And so the other problem is, when you give notice at time of collection, you can only say to people, here's what we're going to do with the data as we can think about it today. But what happens in the future when great uses of data become available because of better technology? Do you really want those uses not to happen? Do you really want to not exculpate innocent people in jail because no one was given notice at the time their blood was taken that DNA may exculpate innocent people and confirm who is guilty, because when that blood was taken there was no DNA. Therefore, there was no notice.

And in all sorts of circumstances, you look at search data, you can look at the search data now and see that people are searching for various drugs and do these drugs have an interaction together that the medical community was not aware of? Suddenly you have a great insight that can save lives. But no one may have thought of that at the time the data was collected. So you have to start thinking about different models, which is very challenging.

So what is the path forward? It is not that collection becomes irrelevant. Collection has huge prophylactic value. If you're worried about the government, for example, misusing data, if you prohibit the collection, then it cannot be misused. So collection has a place. Notice and choice, the idea of user involvement has a huge place. Certainly if I'm collecting data from you, particularly sensitive data like health data, absolutely you should be involved in the process.

The challenge is that the system is now so weighted to the elements that you can't liberate data for other uses, and you are burdening the user in ways that are just intolerable, and causes them to just click and move on without really paying any attention.

The idea that if you tell me you want to buy shoes from me, and I say I need your address to ship the shoes, and I've got to explain to you that I need your address to ship the shoes, you probably figured that out all by yourself. So what things do we really want to engage users on, and what do we want to tell them? And then how do we then say, okay, in that new model, if you're going to have a situation where there will be uses of data where the user of the data isn't going to point to the data subject and say, hey, you can send it, then

what becomes the model, and how do you do those things? And so you start thinking about accountability models for data use. You start thinking about people do collect data, they think of innovative uses for data, but how do we decide if those data uses are okay or not?

And so I came up with a graphical model to think about this that actually applies in a whole range of circumstances. And I actually did this when I was rethinking the cyber threat. Years ago I wrote a paper on what cyber threats we really wanted to combat. And I said there were four, there was cybercrime, and economic espionage, military espionage, and cyber warfare. And these all pose different problems.

Cybercrime, everyone knows what to do. Let's all get together find the criminals and put them in prison. Governments, industry, civilians, everybody wants to do that. In other areas, like economic espionage, there's conflict. Some countries do it, some countries don't. And you don't have normative behaviors. And cyber warfare, people don't even know what it means, so we have to figure out taxonomies.

I went through this, and then the Snowden allegations came out, and PRISM hit. And it became clear that those four buckets weren't quite right, and the reason for that is states. Even states that do not do economic espionage, that is steal data from companies and give it to domestic companies to help them compete, even companies that don't do that economic espionage do spy on other governments for economic data. So if you're going into trade negotiations and want to know the bottom line of the other party, you steal information about their trade positions. It's economic data, but it's not economic espionage in the sense of helping domestic industry out-compete.

And then we had all this surveillance to stop terrorism. And you go, well, that's not economic espionage, it's not military espionage, it's not cybercrime, it's not cyber war, it's something else. So I started thinking, well, what model works for this new environment? And as I built out this model with Jeff Jones, who is sitting here, we built out this model and said, it applies to privacy, too. And it's interesting to just look at the model and then think about how to live in this new world.

There's really always four things, actors, objectives, actions and impacts. So if you think about those things in that way, let's walk through some examples, and you see how it works. So the actor might be the government, and the objective is they don't want planes to blow up. So they take an action. The put in metal detectors to find guns. The impact, people have to walk through a metal detector. Planes aren't blown up. Society says, we're good with that.

Then we had the problem of liquid explosives. So the government gets X-ray machines. And so the government, trying to stop planes from being blown up has a new action, X-ray machines. What's the impact? Well, if you're of my generation, you know that if you're exposed to radiation Godzilla attacks Tokyo. And as a result of that, you go, oh, no, I don't want radiation. Radiation is bad. And there is this backlash. So they come up with back scanner machines, radio waves. So the same government, same objective,

different action. People are okay with back scanner because it's not radiation, which has a bad rap.

So now you start thinking about other things like economic espionage. Foreign government breaks into U.S. companies to steal their IP to help domestic industry. You go, you know what, that's a bad objective. It's just wrong. Because the objective is wrong, whatever action you do is wrong. You're done.

And then you can start thinking about counter-terrorism and privacy. So the actor is the U.S. Government, their objective is to stop terrorist attacks. We all think that's a good objective. So you don't stop there. So what action do you take? Well, you snarf up the world's data, perhaps. What's the impact? And you do an impact assessment. And it's been very interesting to watch that, because that's really what this is all about. The government says they stopped 54 terrorist events, a certain number domestically, a certain number internationally. We go, that's a good impact.

But it's not the only impact. There's an impact to privacy. There's an impact to global competitiveness. There's an impact to living in a surveillance society. We don't like that. And you can start saying, based on what the objective was and the actions taken, we think the bad impacts overweigh the good ones. Which is why Microsoft has come out and said, we don't believe in the collection of bulk data.

You also have to appreciate if the impact were different, we'd be in a different place. Suppose because of all this surveillance they stopped three dirty bombs from going off on the same day, one in Berlin, one in Tokyo, and one in New York? Would we be having this discussion? I suggest it might be a very different discussion.

The point is this model works. And now you can take a company like Microsoft, and we have an objective, to personalize services to our customers. What action do we take? We collect and analyze data, and then we do something like targeted advertising. You say, well, what's the impact? And you do an impact assessment. If we realize you like shoes, and we sent you an ad for shoes, you might say okay. If we said, oh, you might be pregnant, and we sent an ad to your father about a pregnancy, you might say not so good. But this is the model that we have to live with because it's a workable model which allows us to assess risk.

So let me close by saying, look, we always, always have challenges. We've had them forever. We had them in the industrial age in global warming. We have it in the IT age with surveillance. And I actually remain optimistic. Why? Two reasons. On one hand, if you're not optimistic, what are you going to do? Throw up your hands? But more importantly, I'm optimistic because we have had hard problems before and we have managed to solve them. You can go back to time immemorial, society has always been confronted with challenges. We have to build consensus, think through the problems, come up with a plan and execute the plan.

If you go back ten years ago, people would say Microsoft makes the most vulnerable products in the world. Everyone is attacking Windows, NIMDA, Code Red, Slammer, worms everywhere. The Internet keeps going down. We haven't had a major worm in years. It's not that it can't happen, or course it can. But we did a lot of hard work to reduce vulnerabilities in code, build defense in-depth technologies, do things to make people say, we're living in a new world with big data. We're living in a world with terrorists and government surveillance. We have to figure out what we want this world to look like, and then we need to execute against our plan.

Enjoy the conference, and thank you so much.

(Applause.)

END