The John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 4 Article 11

Spring 2015

Legal Problems in Data Management: Global Approach to Data Privacy: Safe Harbor, 31 J. Marshall J. Info. Tech. & Privacy L. 633 (2015)

SESSION SEVEN:

GLOBAL APPROACH TO DATA PRIVACY: SAFE HARBOR

MODERATOR:

DAVID SORKIN
PROFESSOR, THE JOHN MARSHALL LAW SCHOOL

PANELIST:

KIT BROUGH
CERTIFIED INFORMATION PRIVACY PROFESSIONAL(CIPP),
REGULATORY SPECIALIST, GROUPON, INC.

PROFESSOR SORKIN: For our next session, we're going to start with a Global Approach to Data Privacy: Safe Harbor. Our speaker is Kit Brough of Groupon.

MS. KIT BROUGH: Hi. As he said, my name is Kit Brough. I work at Groupon, a Chicago start-up I'm sure you're all familiar with. I am a certified information and pricing professional, a certification you get through the IAPP, which is an organization based in Manchester -- sorry, Portsmith, New Hampshire, and they have huge conferences. They are kind of the leading force in privacy right now. It's an interesting mix of people who are members. It is about half lawyers, half people that aren't attorneys, and you will find that people with the IAPP certifications are a mix of people that sit on legal teams for corporations and people that are actually more IT and info. tech information security focused.

So that's a little bit about my background and what I do. I am on Groupon's legal team, but I'm not an attorney. I'm just an information privacy person.

Okay. I will be speaking about Safe Harbor and feel free to raise your hand at any time with questions, and I will be happy to answer them.

Safe Harbor is a self-regulatory framework. It allows companies in the United States to process the data so that it's in the EU, it's crucial for multi-national corporations to have the certification, the easiest way to transfer data across different countries between the U.S. and EU.

So as I'm sure you're all aware, the EU Data Protection Directive sets out a set of standards that are much stricter than anything that exists in the United States. Safe Harbor is the means of bridging the gap between the two.

The directive went into effect in 1998. It set out privacy as being the fundamental right of citizens of the EU. It is very different than obviously the U.S. where privacy is considered a fundamental right. Obviously, so it's Swiss. Switzerland is not a part of the EU, but there is a separate Safe Harbor certification, separate but yet completely the same, same website, same form you fill out. You just check an extra box if you're dealing with Swiss data.

There are Safe Harbor principles, and I will get into how companies make sure that they are abiding by these principles to keep their certification in check.

So the first principle focuses on the consumer. Notice, you have to let the consumer know which data you're collecting, why you're collecting it, how you intend to use it, and provide choice. The choice can be, you provide the data or you don't provide the data. You use my website or you don't use my website. You buy something; you don't buy something, because, obviously, if you're making a purchase on an eCommerce

site, certain data has to be processed. If you want something mailed to your house, obviously that company has to take your address and then mail you something.

So the choice can be -- it doesn't have to be complicated. It can be use, yes, you use this site, or no, you don't use this site.

The main principle is how the data controller processes and tracks that data. So there's a -- on a transfer, you have to make sure whenever you're transferring data, you have state or contractual policies in place or they are Safe Harbor certified, as well.

You have to make sure that if you bring on third parties that are handling or touching this data in any way, shape, or form, that it's going to be at the same level of protection as if it was still handled by your company. Dealing with vendors is a great chance for something to go terribly wrong.

Security, which is making sure you have basic security in place, you should be -- no matter what, you should be working closely with your own company's security team, protecting against any sort of hacking or malware or misuse.

Data integrity involves allowing consumers to review and correct their information. We get requests like this all the time, where people say, I got to change my last name or I moved, and a lot of that is also providing a website where they can ask questions. So that's why you'll find on most privacy statements, there is a website where people can direct their privacy-related issues.

There's s also CS, customer service e-mails listed where they can make requests to change their personal information.

Access relates to who can actually -- who can view, use, or change, in any way, shape, or form access that data. So a problem that a lot of start-ups find is that they start so small and if everyone needs everything because -- everyone is doing everything.

A few years later, these companies grow and people have access to things they don't need anymore. People should only be accessing the data they need to accomplish their job.

So, for example, somebody on the customer service team doesn't need to be accessing financial information or somebody's salary information. Everything should be segmented, roles should be defined, access for each role should be defined, and it should be audited regularly.

Enforcement, the data controller needs to ensure that the data is only used for a specified purpose. So if you go back to the notice and choice, you're defining how that data is being used.

In the EU, you cannot take that data if you are collecting somebody's e-mail address to send them a confirmation that their order was shipped, you can't take that e-mail address and use it for some direct purpose. That's a huge risk, because it's very clear that it's not allowed.

So a lot of times, once people get their hands on data, they want to

keep it. The tendency is to want to hang on to it just in case, just in case they want to use that phone number later to send a text message or e-mail address to do something else. A lot of the ways I find to protect the Safe Harbor certification and to protect the enforcement element of it is to purge data and to use it for its purpose and when the purpose is over, if it's not an ongoing account-related data collection, to get rid of it.

If we collect a phone number, it's a very specific reason why. Once that purpose is done, you don't need it, and then get rid of the risk of somebody just going rogue and taking it and using it.

I think I've covered most of this already, but the bottom line is that companies need to be handing EU PII with the same care that it receives in the EU. You'll hear again and again, call it notice, choice, and consent.

One thing I always tell people is, we can do whatever we get permission to do. If we want to use data for X purpose, create a checkbox, tell them this is what we want to do, get consent. It sounds so easy, but, like I mentioned before, it can actually be really hard.

You will be talking to people, like what are you developing with this? I already did this for the United States. This is Europe. It's different. You have to make sure that you're protecting data in the same way that it would be there, even if it's finding something in the U.S., you have to treat it separately.

A lot of companies find ways of publishing offers to you. There are certain systems that find heavy U.S. version and the EU version, and by keeping them separate you're able to hold-out in the same Safe Harbor, the protections that Safe Harbor requires.

Working with any vendors to make sure that you're their Safe Harbor certified or that they will execute standard contractual clauses and this is something that a lot of big companies just have in their MSA. That's saying the company's agreeing to execute SCC's if we request.

So there are so many little things that go into Safe Harbor compliance. I run Groupon's annual audit, and it has such a wide range of people that I deal with. I talk with every -- almost single team, whether it's engineering, finance. I work really closely with the audit team. I work really closely with our data engineers and sales and pretty much everyone.

So one of the things that I'm in charge of is the access controls. So you -- the best scenario is to create a system to manage access requests and to log who has access to what so you can review it and audit on annual basis.

Another thing that I look out for is using access management systems, so we have different tools, a single sign on, and by using those tools, we can shut off access when somebody leaves the company. Sometimes that is something that people don't think about. You don't want to have a tool that requires somebody to go in and manually shut off ac-

cess when they leave the company, because that might not happen.

It is so much easier. Everybody just plugs into a system. HR says, they're no longer here, and everything shuts down. So that's something I really look for. Then there is a lot of auditing that has to go on an annual basis, because there is just so many -- especially with start-up culture, people just switch times all the time. So somebody might have been finance and now they're in audit and they need access to different things, but were there a signal through the system to say, this change in role requires change of access. So you're trying to catch all the little things when you do an audit.

Then establishing data retention policies and making sure that people comply. We have a general policy. Everyone's trained on it, and training is a huge part of Safe Harbor. We have established annual training procedures for the entire company where everyone has to go through training and they get reminded of a wide variety of different policies ranging from whether they are a data retention policy. There are guidelines for dealing with CEDA.

There are data access control policies. So we make sure that everyone on an annual basis is reminded of what the policies are, how they apply to the employees, and that they actually check off saying that they have read them on an annual basis.

Then another thing is to provide just-in-time notices and provide accurate privacy policies, so most companies only try to update their privacy policy on an annual basis-ish. People try not to update it too often, so you will find it's usually about a year, sometimes every 18 months or so. But there might be changes that occur in the data processing or the data use in that time period in between, and that's where just-in-time notices can be a huge help in providing notice and choice and consent to the consumer.

So that takes working with the engineering teams and the product teams to understand what the product is, which data they're collecting and how they're using it, and then create a pretty easy, seamless explanation, a short one always, because you have to think about mobile. That fits on a little screen and says this is what we're doing, this is how we're using your data and can we do it.

So there are a lot of different things that come into play when it comes to making Safe Harbor. It's not just an annual audit. It is also constantly talking to product and engineering, understanding what they're trying to do, and making sure that they know when they're trying to create some new product that I'm moved in to make sure that they are not doing anything that conflicts with our existing policies or our current financial statement.

When it comes to Safe Harbor certification, it's the actual form and procedure. It's super simple. It's as easy as filling out a form online and mailing a check. It's everything that comes up to that that is challeng-

ing, because you need to make sure that you have created the right procedures to support the actual certification. Self-regulatory framework, the FTC does have the ability to enforce. So if you are clearly not abiding by the regulation, there could be fines involved. But it's an inexpensive fee. It's online and every single year it's literally just clicking a button to renew. Check when you click the button. Real easy.

So the reason for certifying is, like I said, to allow companies to transfer data internally from the EU and Switzerland to the United States, which is essential for big companies that are trying to centralize operations. So things like HRS functions, a lot of companies use one single system that exists on one single server in one country, and usually that is in the United States.

Engineering functions. There are so many functions that Groupon and a lot of other companies use, we run them out of the United States exclusively, and also data backup systems. A lot of Europeans will have their European server backed up to the United States. Data is everywhere. But if you are a small company not that's accessing -- that's not operating in the European Union, if you're not touching that data or somehow you're operating completely separately and there's nobody in the -- there's no cross-country, cross-border teams, you wouldn't necessarily have to certify if everything was completely separate. But I think that's pretty rare. I think most companies, if they're operating in the EU and in the U.S., there is sort of transfer of data that is occurring.

The other people touched on this quickly, but there is a huge current state with Safe Harbor. Country has made clear that they are not okay with it, that they don't think it's efficient and it's hotly debated. But at this point it seems like although countries might not be thrilled with it, it doesn't seem to be going anywhere right now. There is the risk of potentially getting changed once the regulation is in effect, because that will provide some easier alternatives to Safe Harbor. It will be easier, potentially, for companies to get binding corporate rules at that time, which are overarching. It's a stronger means that that company can adhere to, and then there are also standard contractual clauses -- that each entity can enter into with each other.

I think that's all I have.

Does anybody have questions about Safe Harbor? Yes.

FROM THE FLOOR: Without getting much into proprietary stuff, what have you found is the easiest way to compile and maintain the documentation that you need to support a Safe Harbor certification, and how do you go about verifying annually that it's still accurate and up-to-date?

MS. BROUGH: There's a lot of ways I do that. We have an Internet system, so we keep a lot of policies there centralized. We also distribute

certain notices to employees in the EU. So I work closely with the HR team. In order to give notice and consent, we need to tell our employees that their personal data might be processed out of the United States. It might hit the United States at some point, so we take a lot of steps proactively to provide notice in that way to our own employees. When it comes to consumer data, there are a lot of steps. For me, it's really just getting in the conversations, keeping spreadsheets of who does what, who the contacts are and different teams, poking my head into meetings constantly saying, what are you doing and working a lot with this. It's a lot about establishing really big connections with key coworkers.

Audit and I have a really good relationship and they know when to loop me in, and product knows when to loop me in. The product team is in charge of developing and innovating new products locally.

Does that answer your question?

FROM THE FLOOR: Yeah, thank you.

MS. BROUGH: All right. Thanks, guys.

(Applause.)