METROPOLITAN
CORPORATE
COUNSEL®

FEBRUARY 2016 WWW.METROCORPCOUNSEL.COM

MCC GUIDE TO IN-HOUSE TECH

MCC INTERVIEW: Jessica Lockett & Alison Wisniewski / Epiq Systems

Identifying the Implications of the *Schrems* Decision in Canada

Connecting the dots on data transfers between Canada, the EU and the U.S.

On October 6, 2015, Europe's highest court, the European Union Court of Justice (CJEU), issued the Schrems *decision, invalidating the EU Commission's Safe Harbor program, which had allowed for legal data transfers between the EU and the U.S.* ***Jessica Lockett*** *and* ***Alison Wisniewski*** *from* ***Epiq*** *– a leading global provider of technology-enabled solutions for eDiscovery, document review, bankruptcy and class action administration – explain the decision's immediate effects on Canadian organizations, as well as contemplate the likelihood of disruptions down the line. Their remarks have been edited for length and style.*

MCC:* Schrems' *immediate impact in the U.S., a party to the Safe Harbor program, was significant, particularly for technology and other companies that relied on Safe Harbor. Canada, however, was not a party to the program. Does that mean data transfers are permissible and the decision has no impact in Canada?

Wisniewski: Correct, the EU decision doesn't currently have any impact on Canada or data transfers in Canada. There may be some issues if the data being transferred from Canada to the U.S. contains personal information of EU citizens.

Lockett: It is important to understand why Canada was not a party to the Safe Harbor program. The privacy protections in Canada were deemed adequate by the EU such that Canada didn't need to participate in the Safe Harbor program. That's the reasoning behind Canada's nonparticipation and the lack of impact of the *Schrems* decision in Canada.

Privacy protections in Canada were deemed adequate enough by the EU such that Canada didn't need to be a participant in the Safe Harbor program.
– Jessica Lockett

MCC: Can you clarify how transfers between Canada and the U.S. are undertaken?

Wisniewski: Canada already has its own data protection act, the Personal Information Protection and Electronic Documents Act (PIPEDA), whereby there are certain requirements in the U.S. that must be followed in order to transfer personal information from Canada into the U.S. It is similar to what is needed in the EU, such as consent from the parties from whom we're collecting personal information, and sometimes consent to transfer such data into the U.S., actual explicit consent. Under Safe Harbor, the U.S. was able to conduct transfers from Canada into the U.S. without obtaining consent. However, even when Safe Harbor was recognized, clients in Canada typically would require that we obtained consent from the data subjects prior to the transfer of personal information from Canada to the U.S. Therefore, the requirements to transfer personal information from Canada into the U.S. haven't changed, unless Canada is transferring EU-specific personal information. In such an event, certain other precautions are needed in order for Canada to make that transfer.

MCC: The EC's* Schrems *Safe Harbor decision affects the transfer of personal data from the EU to the U.S. What does that mean for Canadian organizations that transfer EU citizens' data to U.S. territory or store or host it within the U.S.?

Wisniewski: Canadian organizations that transfer, store or host EU citizens' data could face some issues when transferring such data into the U.S. because Safe Harbor is no longer recognized by the EU. If we were transferring EU personal data into the U.S., the Safe Harbor protections would not apply. We have started entering into standard contract clauses with clients in the EU that allow the transfer of personal information back and forth; we sign that as a data processor. This might be something we would now need to consider with Canadian organizations in order to transfer personal information into the U.S. Epiq currently has a facility in Canada to host and process data, though, so EU citizens' data could remain within Canada and not have to come into the U.S. for any service that we provide.

Lockett: I agree. Generally, organizations such as Epiq that have the capability to host, store and process data within Canada are going to

Jessica Lockett
Director of Document Review Services in Toronto at Epiq Systems.
jlockett@epiqsystems.com

Alison Wisniewski
Vice President, Corporate Counsel at Epiq Systems.
awisniewski@epiqsystems.com

epiq SYSTEMS

be able to work around that concern with respect to the transfer of EU personal information into the U.S. If they're able to hold data in Canada, the personal information protections currently afforded by Canada's laws are deemed adequate by the EU.

MCC: Are there specific steps that Canadian organizations transferring EU citizens' data should take in anticipation of what some observers say could be ripple effects from the* Schrems *ruling?

Wisniewski: For Canada, because its privacy act was drafted with the EU Data Directive in mind, and because it was not affected by the *Schrems* ruling, EU organizations can continue to transfer personal data to Canada as they have been without any impediment, unless and until the EU decides to take a look at PIPEDA and make changes.

Lockett: The ripple effect could be a concern in terms of a potential re-examination into Canada's privacy laws. It's been almost 15 years since PIPEDA was deemed adequate protection by the EU. It hasn't happened as of yet, but it leaves open the possibility that the EU could re-examine Canada and other countries' privacy laws to determine whether they still maintain adequate protection for EU citizens' data.

MCC: Although PIPEDA, which as you mentioned was motivated partly by the EU Data Directive, was determined to provide an adequate level of protection for the purpose of data transfers from the EU to Canada by the EU Commission in 2002, the European Parliament Committee on Civil Liberties, Justice and Home Affairs called for a review of Canada's privacy protections during its membership in the Five Eyes Alliance. It remains to be seen whether Canada will be challenged on the basis that it no longer provides adequate protection for EU citizens' data. What might the implications be?

Epiq has a facility in Canada so EU citizens' data can remain within Canada for any service that we provide.
–Alison Wisniewski

Wisniewski: We would have to see how they rule. If they don't re-approve it, like they didn't approve Safe Harbor, then either Canada would be in the same position as the U.S. when it comes to personal data transfers to the EU, or Canada could revise the PIPEDA to reflect whatever comments the EU had in order to remain in line with the EU Data Directive. It depends on the decision.

MCC: Is there any talk in Canada about trying to get in front of a prospective review?

Lockett: The *Schrems* decision is still new, and I haven't heard of any discussion, at least from policymakers, on its specific effect on legislation in Canada. However, the federal Anti-terrorism Act, 2015, Bill C-51, was recently passed by Parliament. The act has potential impact on the Canadian government's reach into personal data within Canada, and also makes some changes to Canada's broader privacy laws. Companies should be aware of these issues and get a plan in place on how to deal with different outcomes with respect to any re-examination of PIPEDA by the EU. It's a little too unknown at this point, but being mindful and watchful is important.

MCC: Some experts have cautioned against underestimating the implications of the CJEU's judgment in* Schrems*, which they say could undermine mechanisms sanctioned by the EU to transfer data to the U.S., including contractual language and even the ECU's decision that Canada's federal data protection law adequately protects EU citizens' personal data. Are we on a slippery slope here, given the EU's hardline approach to privacy?

Wisniewski: By not allowing a reliance on Safe Harbor, it makes it much more difficult for the U.S. to conduct business in the EU. There are lots of different contractual requirements that will be required under agreements, as well as other requirements such as having a data center locally, having the capability to provide all of the services that a technology company provides locally, and actually being physically located in the EU. For Canada, that's not much of an issue right now, because they're not affected by Safe Harbor. In the event Canada is affected by an EU ruling of PIPEDA, more organizations will have to focus their services locally in the EU, adding expense and resources, rather than conducting a more global business.

Lockett: That's a great point. Europe appears to lead the pack in privacy protection, and they're coming out with a hard stance. It's not necessarily a bad thing, in my opinion, but legislators will somehow need to strike a balance between promoting commercial activity in a global market, and upholding the privacy protection of individuals.

MCC: For the companies doing business in Canada that you're working with, are you involved in any contingency planning right now for any disruption if things do change? The expectation is that changes need to be executed fairly quickly when working with the EU.

Lockett: There's been no discussion with clients of mine, but like I said before, people should be alive to the issue. There may be less of a concern with our clients, because we do have operational capabilities for hosting and processing in Canada, so Epiq currently has an extra protection there for our clients.