The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2015
PHILADELPHIA, FRIDAY, NOVEMBER 6, 2015 VOL 252 • NO. 92 An ALM Publication

E-DISCOVERY AND CYBERSECURITY

Data Storage After the EU Safe Harbor Decision

BY JANA LANDON

Maksim Kabakou/Fotolia

In early October, over 4,400 U.S. companies collectively held their breath in anticipation of a ruling from the Court of Justice of the European Union in the Schrems v. Irish Data Protection Commissioner (Case C-362/14) matter. This case would decide whether or not the data safe harbor agreement (DSHA) penned in 2000 and governing transfer and storage of personal data of EU citizens on U.S. servers was valid. It threatened to undo over a decade's worth of a data privacy framework that many companies, including multinational corporations, social media outlets and cloud providers, had relied upon when facilitating Trans-Atlantic business.

In an unprecedented decision issued Oct. 6, the EU court invalidated the DSHA, sending companies into uncharted waters as they now attempt to determine what the ruling means and what port they should now dock in to find "adequate protections" for this data that would comply with EU law.

What Was the Data Safe Harbor Agreement?

Ratified in July 2000, the DSHA allowed for the passage of personal information about EU individuals between the EU and the United States as a matter of commerce, as long as U.S. data custodians ensured adequate protection of such sensitive data. While those in the U.S. data security field often think of "personal data" as personally identifiable information (e.g., financial information) or personal health information (e.g., medical records), the EU has, historically, taken a much wider view, defining it as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

This would include such information as Google searches, Facebook posts, information on an individual's Netflix accounts, and a million other data points that many companies gather from their customers and sell.

Any U.S. company could self-certify under the DSHA that it adhered to the U.S.-EU Safe Harbor Framework developed by the Department of Commerce in coordination with the European Commission, the EU's executive body, and thereby provided "adequate protection" of EU data. All self-certifying companies were listed on the Department of Commerce's website, and could be removed if an enforcement body found that an organization had not been complying with the U.S.-EU Safe Harbor Privacy Principles. Companies had to reaffirm their self-certification yearly.

Enter Edward Snowden. In 2013, he leaked information regarding the National Security

Agency's practices, disclosing that American and British intelligence agencies had almost unfettered access to data stored on U.S. servers, including data of EU citizens. The European Commission issued a communication shortly thereafter titled "Rebuilding Trust in EU-US Data Flows," which specifically called out its concerns with the DSHA and provided 13 "recommendations" for the DSHA, without any clear guidelines as to how these would be enforced.

The United States and EU have worked for over two years to address the concerns voiced by the EU in 2013 and negotiate a new safe harbor agreement. Talks have stalled, according to news reports, over what type of access to European data American intelligence agencies should be given. Additionally, the EU has been pushing for EU citizens to have the right to sue U.S. companies for privacy violations. While negotiations regarding what has been referred to as "Safe Harbor 2.0" are continuing, the House of Representatives has already passed the Judicial Redress Act of 2015, and it is on its way to the Senate.

The Schrems Complaint

Snowden's revelations also played prominently in the complaint filed against Facebook in Ireland by Maximillian Schrems, a 27-year-old Austrian graduate student and activist.

Any person residing in the EU who wishes to use Facebook is required to sign an agreement with Facebook Ireland, a subsidiary of Facebook Inc. Some or all of the personal data of Facebook Ireland's users who reside in the EU is transferred to servers belonging to Facebook Inc. that are located in the United States. Schrems argued in his complaint that Europeans' online data was misused when Facebook was said to have cooperated with Prism, a program run by the NSA that specifically targeted foreign nationals' data. He requested that the Irish data protection commissioner instruct Facebook Ireland to keep his data within the EU.

The commissioner, relying on the DSHA, stated that he did not need to investigate this complaint and rejected it as unfounded, stating that there was no affirmative evidence that Schrems' data had been accessed by the NSA, and further, that the European Commission's approval of the DSHA showed that the United States maintained an adequate level of protection for relevant data.

Schrems appealed to the High Court of the European Union, which subsequently found that the DSHA "enables interference, by United States public authorities, with the fundamental rights of persons" and invalidated the law. It instructed the commissioner to review Schrems' complaint on the merits.

Ramifications of the Decision

With the DSHA invalidated immediately and no grace period noted in the decision, as of Oct. 6, the state of EU data on U.S. servers was unclear. In a statement issued 10 days later, a group of data protection officials representing 28 EU member states offered a small reprieve but did nothing to further allay many companies' fears of a wave of EU enforcement actions. The Article 29 Working Party on the Protection of Individuals affirmed that any transfers being made to the United States on the basis of the DSHA were unlawful, and they reserved the right to investigate any privacy complaints that arose in relation to transfers if the European Commission and the United States did not agree on a "Safe Harbor 2.0" by the end of January 2016, thereby increasing pressure on U.S.-EU negotiations and Congress. The EU has added further fuel to the political fire by passing a resolution to protect EU personal data from surveillance; members of the European Parliament have also called on EU member states to grant Snowden asylum as an "international human rights defender."

The Oct. 6 decision may be the beginning of a domino effect among other countries that have looked to the DSHA as a guide for their dealings with the United States. On Oct. 19, the Israeli Law, Information and Technology Authority revoked its prior authorization for data transfers from Israel to the United States. Israel's Protection of Privacy Law states that a citizen's personal data cannot be exported to a country that has a weaker level of protection than that guaranteed by Israel; the 2001 law permitted its companies to self-certify whether a country was considered "safe" under the DSHA.

What Happens Next?

Importantly, the Schrems decision merely remanded the complaint to the commissioner, meaning that there was no finding that Facebook broke any EU law. Instead of giving the power to an overarching EU governing body to decide whether or not laws were violated, however, it places the decision squarely with the supervisory authorities of EU member states such as Ireland, which may lead to a "patchwork" of privacy laws. Therefore, it will be important for U.S. companies storing EU data to know exactly which countries' data privacy laws affect them, if a new and improved DSHA is not implemented.

Further, the decision gives companies the impetus to make sure that they are adequately protecting foreign data. The Article 29 Working Party noted in its Oct. 16 statement that alternatives to DSHA, such as model contract language or binding corporate rules, are still available to companies. From a practical perspective, any company that houses EU data in the United States, either directly or through a vendor, should examine its contracts carefully to ensure compliance with EU rules. If vendors were previously DSHA-compliant and state that they now comply with all EU privacy regulations, U.S. companies should consider additional contractual language regarding legal and administrative remedies if, indeed, investigations and enforcement actions from EU authorities occur.

Finally, it is important to remember that an EU citizen can authorize the transfer of his or her data under certain circumstances—companies may want to consider adding appropriate language to their agreements.

Of course, companies can also decide to segment certain data to reside within the EU, but this may create inefficiencies and impediments to operations. While U.S. organizations can hope that the United States and the EU agree on a new safe harbor agreement by the end of January 2016, it appears that the data security waters will be choppy until at least then.

Jana Landon *is counsel in Stradley Ronon Stevens & Young's Philadelphia office and founder and chair of the firm's e-discovery team. Her practice focuses on advising lawyers and clients on legal, technical and strategic issues regarding cybersecurity, electronic discovery and information governance, as well as representing clients in complex insurance coverage matters. She can be reached at jlandon@stradley.com or 215-564-8049.*

Reprinted with permission from the November 6, 2015 edition of THE LEGAL INTELLIGENCER © 2015 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382, reprints@alm.com or visit www.almreprints.com. # 201-11-15-05