Bloomberg BNA

Privacy and Security Law Report®

Data Transfers

Views on the Invalidation of the U.S.-EU Safe Harbor From James H. Koenig, Of Counsel, Paul Hastings

Thousands of U.S. companies that relied on the U.S.-EU Safe Harbor Program to transfer personal data out of the European Union received a shock when the EU's top court invalidated the program (14 PVLR 1825, 10/12/15).

Bloomberg BNA Privacy & Data Security News Managing Editor Donald G. Aplin posed a series of questions to James H. Koenig, of counsel in the Litigation Department at Paul Hastings LLP in New York, about the ruling and what companies should do now.

Koenig was a panelist on a recent Bloomberg Law webinar on the demise of the Safe Harbor Program. The archived webinar is available at http://www.bna.com/european-court-justice-m57982059673/.

BLOOMBERG BNA: Did the European Court of Justice opinion's focus, scope or language surprise you in any way?

James Koenig: The ECJ's decision in *Schrems* was surprising in that it went beyond the narrow question presented by the Irish High Court—namely whether the Irish Data Protection Commissioner (DPC) was bound by the European Commission's (EC) July 2000 decision (2000/520/EC) finding that the privacy principles of the U.S.-EU Safe Harbor accord provide an adequate level of protection of the personal data of EU citizens, or whether the DPC could—or is even required to—conduct its own investigation in light of intervening factual developments.

In addition to determining that the Irish DPC had such authority, the ECJ went further, itself declaring that the EC's prior adequacy decision was invalid. The consequences of this broader holding were great and left the approximately 4,400 Safe Harbor-certified companies without a legitimate basis to transfer personal data from the EU to the U.S. Much of the resulting uncertainty may have been avoided had the ECJ limited itself to answering the narrow question presented. The decision highlights the inadequacy of the ECJ's attempt

 ISSN 1538-3423

to provide a judicial solution to what many believe is, at its core, a diplomatic and trade issue.

BLOOMBERG BNA: What should companies that were relying on the Safe Harbor directly—or on vendors that were self-certified—do in both the short and long term to seek lawful ways to transfer data out of the European Economic Area?

Our advice to clients is to keep calm, enhance things and carry on.

Koenig: In response to the decision (and some in preparation for it), clients who have been depending on Safe Harbor to transfer data from the EU to the U.S. (or as the backbone of global transfers) have been taking or considering a number of approaches to minimize compliance and enforcement risks:

1. **Putting Model Contracts in Place (Also Binding Corporate Rules (BCRs) Longer Term)**. Implementing Model Contracts/Intra-Group Agreements (or even outsourcing data storage or certain IT operations to vendors with data transfer mechanisms in place) to cover any data transfer or access gaps they feel they may have (as a longer term solution, some companies are considering binding corporate rules as one additional data transfer mechanism to also put in place);

2. **Reviewing Data Flows and Prioritizing Remediation**. Inventorying what personal data are being stored and transferred and prioritize key data transfer activities that must remain intact (business or operationally critical) and focus efforts toward ensuring data transfer and storage solutions are in place or can be rerouted or stored in a way to minimize risks (or avoid using a Safe Harbor-supported pathway);

3. **Contract Analysis.** Analyzing existing contracts where there could be a breach based on the European Court of Justice opinion (or pursuant to a subsequent determination in an EEA member country), and, in such analysis, prioritizing the relationships and contracts to review data transfer pathways and compliance and/or to identify alternative legal or data architecture solutions;

4. **Considering EU Country-by-Country Leeway**. Identifying where servers in the EU are located, and the specific local requirements and privacy protections, as national authorities will have greater leeway; and

5. **Outreach to DPAs and Monitoring Consumer Complaints**. Reaching out to Data Protection Authorities (DPAs) to build relationships and trust, while also updating consumer complaint and redress procedures to heighten alert to any specific requests or complaints as we expect more individuals to raise issues and concerns around privacy and data transfers.

BLOOMBERG BNA: Given the new higher privacy adequacy threshold announced by the ECJ, might those alternative transfer mechanisms, and even country adequacy determinations, also be at risk of being found invalid?

Koenig: Yes, there is uncertainty about the use of other transfer mechanisms, including model contracts and BCRs, by U.S. companies. Indeed, a consortium of German DPAs have said they would not approve any transfers on the basis of BCRs and that they plan to exercise their audit powers over standard contractual clauses—highlighting the potential need to modify model contract provisions.

A key wild card created by *Schrems* is the issue of governmental surveillance and how that will be addressed through commercial data transfer mechanisms—both with U.S. but also with other jurisdictions—going forward. Although that was never the focus of articulated EU concern with the Safe Harbor in the past, it is an issue that applies equally to all mechanisms that might be used. Moreover, some have said there may be some hypocrisy in the EU stance as its own national surveillance laws can be quite sweeping.

Our advice to clients is to keep calm, enhance things and carry on. Despite the uncertainty, all companies are doing something on a risk basis in light of the ECJ's decision. Some are moving ahead to devise a global solution without awaiting or depending on the promised Safe Harbor 2.0. Others are taking interim measures. The appropriate approach varies, depending on the type of company and the sensitivity of the data at issue. The high visibility of some, such as social media companies, puts them at a higher risk for possible EU regulatory focus. The bottom line, however, is that the *Schrems* decision is forcing all organizations that were part of the Safe Harbor Framework to make risk-based—not just legal—decisions.

The bottom line, however, is that the *Schrems* decision is forcing all organizations that were part of the Safe Harbor Framework to make risk-based—not just legal—decisions.

BLOOMBERG BNA: Do you think the Article 29 Working Party's statement about potential enforcement after the end of January 2016 (14 PVLR 1940, 10/26/15) really represents a meaningful threat?

Koenig: Yes, there is a meaningful threat of enforcement stemming from the Working Party's statement that it would start to enforce the ECJ's decision at the end of January 2016 unless U.S. and EU negotiators had agreed on a replacement mechanism for the Safe Harbor. In addition to the substantial visibility around the Working Party's statement, a number of individual DPAs have begun making interim inquiries. For example, the Spanish DPA issued letters to many companies that had previously notified it of cross-border data transfers that relied in whole or in part on Safe Harbor certifications. The letter asked such companies to inform the Spanish DPA by Jan. 29, 2016, of the new, alternative mechanisms they have implemented to ensure adequate protections for data transfers to the U.S.

  PVLR ISSN 1538-3423

Some Europeans are of the view, however, that the Working Party's statement should be viewed less as a threat than as a means of preventing individual DPAs from bringing individual complaints before the end of January. National DPAs will be sitting on complaints from data subjects and will be eager to proceed with them after the end of January 2016.

The key for companies is that there is likely to be a lot of activity following the January deadline—whether it is enforcement-focused or a combination of investigation and enforcement—which should factor into risk-based business decisions regarding future data transfer.

BLOOMBERG BNA: Do you think there is a realistic chance that EU and U.S. officials will come up with a Safe Harbor 2.0?

Koenig: There are reasons to be optimistic that Safe Harbor 2.0 is forthcoming. Unofficial sources involved in negotiations have indicated that agreement on much of the enhanced framework had already been reached prior to the ECJ's decision. In addition, European Justice Commissioner Vēra Jourová announced recently that there was agreement ''in principle'' between the EU and U.S. regarding components of a new Safe Harbor mechanism.

Challenges remain, however, as the sides seek to address the ECJ's concerns regarding when U.S. public authorities may intervene, including for reasons of law enforcement and national security. Furthermore, even if an agreement is reached, the possibility remains that the adequacy of the revised mechanism could be challenged, leading to another round of litigation before the ECJ.

In the interim, even companies that expect Safe Harbor 2.0 to soon emerge are selectively taking actions such as implementing model contracts, rerouting data flows and assessing primary vendors to manage the risk that the new framework will not be completed by the end of January.

BLOOMBERG BNA: Any creative solutions on the horizon?

Koenig: Yes, we've seen some cloud database and other hosting companies hedging their bets by opening or expanding data centers in Europe. For example, Microsoft announced that it will offer its European customers the option of storing their cloud data in data centers in Germany.

However, if this strategy is pursued widely, it could lead to the Balkanization of the Internet. This Balkanization would mean—instead of a single connected network—a divided internet, broken down by region or by country. This would only be accelerated by the proliferation of more country-based laws requiring citizens' data or other types of data to remain within national borders. For example:

- Russia has already implemented such a data localization law, requiring companies to store and process all personal data of Russian citizens using databases stored in Russia.

- South Korean law has been interpreted, for example, to prohibit mapping data from being stored on servers outside South Korea, limiting the use of applications of GPS and location-based Web applications, such as Google Maps.

- In addition, Canadian provincial laws (in British Columbia and Nova Scotia) require personal information held by public bodies to be stored and accessed only in Canada unless one of a limited number of exceptions applies.

More localization laws may be the future following the *Schrems* decision if regulators and businesses are not careful. At risk here is the potential to lose the opportunity to manage data globally and fully realize the benefits that big data analytics and permission-based global databases can offer—including for health, entertainment and to generally improve our quality of life.

Koenig thanks Behn Dayanim, Ashley Winton and Mary-Elizabeth Hadley of Paul Hastings' Privacy & Cybersecurity Practice for their assistance in responding to Bloomberg BNA's questions.