Skadden

# Privacy & Cybersecurity Update



Four Times Square
New York, NY 10036
212.735.3000

## Court of Justice of the European Union Declares US-EU Safe Harbor Invalid

"Decision 2000/520 is invalid." With those four words, the Court of Justice of the European Union (CJEU) sent shock waves through the European and U.S. business communities on October 6, 2015, with a landmark decision finding that the U.S.-EU Safe Harbor is invalid. For some 15 years, over 4,000 U.S. companies have relied on the Safe Harbor Framework to transfer personal data from the European Union (EU) to the U.S. in a manner that meets the requirements of the EU Data Protection Directive. The immediate impact is as follows:

- **Companies that have relied on their own Safe Harbor certification to transfer data from the EU to the U.S. in compliance with the EU Data Protection Directive must now promptly adopt and implement an alternative means to comply with the directive.**
- **Companies that do not themselves rely on the Safe Harbor but transfer data to U.S.-based vendors who are Safe Harbor certified should ask those vendors how they are addressing this change in the law.**
- **Companies that rely on other means of complying with the directive do not need to take immediate action but should carefully watch developments as they unfold in the EU, since these other means of compliance may soon come under attack as well.**

**The Skadden Privacy and Cybersecurity Group is available to help companies navigate this significant change in European law.**

### Background

Under the EU Data Protection Directive, personal information about EU citizens can only be transferred from the EU to countries with adequate data protection. Only a handful of countries satisfy this requirement, and the U.S. is not one of them. The European Commission has provided a few mechanisms for companies to conduct such transfers if they are not located in a country that meets the adequacy requirement. In the U.S., one of these mechanisms is the Safe Harbor, which was negotiated between the European Commission and the U.S. Department of Commerce and went into effect in 2000. To enjoy the benefits of the Safe Harbor, a company must self-certify to the

Department of Commerce that it complies with specified EU privacy standards. Once the company has self-certified, it can receive personal data from the EU. As a general matter, the Federal Trade Commission (FTC) has enforcement powers if companies violate the Safe Harbor or state they are certified when, in fact, they are not.

### *Schrems v. Data Protection Commissioner*

#### Facts of the Case

In *Schrems v. Data Protection Commissioner*,[1] the plaintiff alleged that Facebook's Irish subsidiary transferred data to the U.S. under the Safe Harbor. Schrems alleged that because Facebook participated in the National Security Agency's (NSA) PRISM program, which allowed the NSA unrestricted access to his data, his fundamental rights of privacy had been violated. The PRISM program became public as a result of documents leaked by former NSA contractor Edward Snowden. While there was no evidence that Schrems' data had been accessed by the NSA, Schrems filed a complaint with Ireland's Data Protection commissioner. The Irish authority rejected the complaint given that the European Commission had already determined that the Safe Harbor ensured an adequate level of data protection. Schrems appealed to the Irish High Court, which then referred the case to the CJEU.

As we reported in our September 2015 *Privacy & Cybersecurity Update*, the CJEU requested an advisory opinion from Advocate General Yves Bot. Bot's opinion harshly critiqued the Safe Harbor as a means to protect the privacy rights of EU citizens given the relatively unfettered right of the U.S. government to access personal information, and concluded that it should be declared invalid. The CJEU adopted all of Bot's conclusions and recommendations.

#### The Court's Holding

The CJEU opinion contains two holdings with far-reaching impact. First, the court held that even though the European Commission may have rendered a decision as to whether a country ensures an adequate level of protection — as it did when it approved the Safe Harbor — individual Data Protection Authorities (DPAs) from member states have "complete independence" to examine the claim "with all due diligence." In the case of *Schrems*, this meant that the Irish data protection authority was well within its rights and powers to question whether the Safe Harbor adequately protected the fundamental right of privacy of Irish citizens. While the CJEU held that only the CJEU itself can ultimately declare a commission decision invalid, its holding gives individual country DPAs wide latitude to challenge commission decisions and then refer the matter to the CJEU. The practical implications of this holding are discussed in the next section.

Second, the CJEU declared that the Safe Harbor was invalid. The court's reasoning closely followed the Bot report. In broad, sweeping language, the CJEU established a high standard for permissible transborder data flows. According to the court, ensuring an "adequate level of [data] protection" for EU citizens, as is required by the Data Protection Directive, means providing "a level of protection of fundamental right and freedoms that is essentially equivalent to that guaranteed within the European Union." The court found that the Safe Harbor failed to meet this standard because nothing in the Safe Harbor stops the U.S. government from collecting and examining the personal data of EU citizens, even if there is no direct national security risk, and EU citizens have no recourse if that happens. According to the CJEU, this violates the fundamental privacy right of EU citizens, rendering the Safe Harbor invalid.

### Practical Implications of the CJEU Decision

- With the Safe Harbor declared invalid, companies that relied on that agreement to send data from the EU to the U.S. must now promptly adopt one of the alternative means available to comply with the EU Data Protection Directive. The most likely alternative for companies is the so-called "model contracts," which are form contracts provided by the EU that are signed by the EU and U.S. entities and include various requirements for how data can be handled and processed in the U.S.[2] For companies that transfer data to the U.S. from only a handful of sources in the EU, this solution may be relatively easy. However, for companies with multiple touchpoints between the U.S. and the EU, this may prove to be a cumbersome and lengthy undertaking. The U.S. Department of Commerce is expected to issue a report in the coming days on how companies should react to the CJEU decision.
- Many companies that currently transfer data from the EU to a processor in the U.S. rely on the fact that the processor has represented that it is Safe Harbor certified. Companies need to review their agreements with such processors, identify which ones have made this representation and promptly work with that entity to find an alternative means to satisfy the EU Data Protection Directive. Similarly, vendors that have relied on its Safe Harbor certification should expect inquiries from their clients in the coming days.
- While the CJEU opinion only concerned the Safe Harbor, the first prong of its opinion gives individuals the clear right to go to individual DPAs and challenge other "adequacy" mechanisms authorized by the commission, such as the model contracts. We expect such challenges to be brought, although it remains to be seen whether the CJEU would have the same negative view of the model contracts as it does of the Safe Harbor.

[1] Case number C-362/14, in the Court of Justice of the European Union.

[2] Other mechanisms for transborder data flow include binding corporate rules (for intracompany transfers) and cases where the individual has given explicit and informed consent.

- The European Commission and the U.S. Department of Commerce have been working closely over a number of months to revamp the Safe Harbor, partly to address the issues raised by the CJEU. Such negotiations will now be further complicated, and perhaps delayed, by the fact that the commission will need to obtain the buy-in of individual DPAs, lest it reach an agreement with the U.S. only to promptly face challenges from the DPAs. Similarly, the EU is currently working toward a new data protection directive — the General Data Protection Regulation (GDPR). Since part of the GDPR will address transborder data flow and the issue of "adequacy," the CJEU decision may delay agreements on that regulation.
- By holding that individual data protection authorities have the power to challenge individual data transfers despite a commission ruling, the CJEU has created the potential for a highly fragmented privacy landscape in Europe — exactly what the Data Protection Directive was meant to avoid. The European Commission is expected to work with the DPAs to address this issue.
- The CJEU decision, along with its May 2014 decision requiring that search engines provide EU citizens with a "right to be forgotten," shows that the court has no problem issuing opinions that have significant repercussions for EU-U.S. commercial activity.

The Skadden Privacy and Cybersecurity Group will continue to closely monitor developments in this important area.

If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

**Stuart D. Levi**
Partner / New York
212.735.2750
stuart.levi@skadden.com

**Cyrus Amir-Mokri**
Partner / New York
212.735.3279
cyrus.amir-mokri@skadden.com

**James R. Carroll**
Partner / Boston
617.573.4801
james.carroll@skadden.com

**Brian Duwe**
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

**David Eisman**
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

**Patrick Fitzgerald**
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

**Todd E. Freed**
Partner / New York
212.735.3714
todd.freed@skadden.com

**Marc S. Gerber**
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

**Lisa Gilford**
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

**Rich Grossman**
Partner / New York
212.735.2116
richard.grossman@skadden.com

**Timothy A. Miller**
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

**Timothy G. Reynolds**
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

**Ivan A. Schlager**
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

**David E. Schwartz**
Partner / New York
212.735.2473
david.schwartz@skadden.com

**Michael Y. Scudder**
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

**Jennifer L. Spaziano**
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

**Helena J. Derbyshire**
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

**Gregoire Bertrou**
Counsel / Paris
33.1.55.27.11.33
gregoire.bertrou@skadden.com

**Jessica N. Cohen**
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

**Peter Luneau**
Counsel / New York
212.735.2917
peter.luneau@skadden.com

**James S. Talbot**
Counsel / New York
212.735.4133
james.talbot@skadden.com

**Joshua F. Gruenspecht**
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com