Pepper Hamilton LLP
Attorneys at Law

CLIENT ALERT

June 8, 2015

Microsoft Warrant Challenge Could Alter U.S.-EU Data Pact

Jan P. Levine | levinej@pepperlaw.com
William M. Taylor | taylorw@pepperlaw.com

This article was published in the Appellate, New York, Privacy, Technology, and White Collar sections of Law360 on June 8, 2015.

The current data privacy debate involving the transfer of personal data from Europe to the U.S. by American companies centers on two competing characterizations. The moral-driven narrative posits that U.S. corporations have no regard for European

privacy concerns or their data protection laws, which enshrine "the basic principle of confidentiality of personal data ... as a human right."[1] The economic-driven narrative, however, posits that Europeans are less concerned about protecting privacy than they are about undermining the dominance of U.S. Internet companies in European markets.

President Obama recently expressed this view, explaining, "In defense of Google and Facebook, sometimes the European response here is more commercially driven than anything else. As I've said, there are some countries like Germany, given its history with the Stasi, that are very sensitive to these issues. But sometimes their vendors — their service providers who, you know, can't compete with ours — are essentially trying to set up some roadblocks for our companies to operate effectively there."[2]

These two narratives have generated dramatic catchphrases and themes: the safe harbor is dead; Europeans have a right to be forgotten; the Stadtpolizei will seize your data. This momentum will be intensified as a result of the following:

- Reforms to the U.S.-EU safe harbor, which will lead to additional regulatory requirements and government enforcement of companies with operations in Europe.
- The EU will expand its application of the "right to be forgotten" law beyond search engines, such as Google Inc.
- The Microsoft Corp. warrant case, where Microsoft's appellate brief features the German Stadtpolizei's hypothetical data seizure, underscores how U.S. government police action may have the effect of decreasing the competitiveness of U.S. companies against European challengers.

Moreover, these challenges have particular significance because they are developing in the context of the EU's overhaul of its data protection framework, with the new laws expected to take effect in 2017.[3] The following analysis addresses these challenges and how they may impact U.S. companies with operations in Europe.

Although Rumors of Its Death May Be Exaggerated, Reforms to the Safe Harbor Will Add Regulatory Requirements and Increase Enforcement Actions

The Safe Harbor's Benefits

Thousands of U.S. businesses rely on the U.S.-EU safe harbor framework for the transmission of personal data from the EU, and it has become crucial to U.S.-EU trade ties. Directive 95/46/EC (Data Protection Directive) provided the impetus for the creation

of the safe harbor by setting rules for the protection of EU citizens' personal data and the transfers of such data from the EU to countries outside the EU, including the U.S.[4]

The Data Protection Directive prohibited the transfer of EU citizens' personal data to countries, including the U.S., that do not ensure adequate levels of protection for personal data. In 2000, the European Commission and U.S. Department of Commerce reached agreement on a program (i.e., the safe harbor) to meet that adequacy standard. To participate in the voluntary program, "a company must self-certify annually to the Department of Commerce that it complies with the seven privacy principles required to meet the EU's adequacy standard: notice, choice, onward transfer, security, data integrity, access and enforcement."[5]

The participation in, and benefits of, the safe harbor have been robust. According to the Department of Commerce's website, more than 5,000 companies have participated in the program, and approximately 4,258 companies currently self-certify their compliance with the program.[6] These companies include "well-known Internet companies and industries ranging from information and computer services to pharmaceuticals, travel and tourism services, health care or credits card services."[7] Officials in the U.S. and EU recognize its importance to both economies.[8]

Enforcement

The safe harbor has enforcement mechanisms in both the U.S. and EU. In the U.S., the Federal Trade Commission is responsible for enforcement, and does so pursuant to Section 5 of the Federal Trade Commission Act. From 2009 through 2014, the FTC brought 24 safe harbor cases based on alleged misrepresentations by U.S. companies that they were in accordance with the safe harbor agreement.[9] From the EU side, the EU national data protection authorities are permitted to suspend data transfers to safe harbor-certified companies, but they have never done so.[10]

The Safe Harbor's Failings and Rumored Death

According to some EU data protection authorities, the U.S. safe harbor program is not sufficiently transparent or effectively enforced.[11] Their transparency and enforcement concerns arise from the perceptions that: (1) the program is inherently weak because it is voluntary and relies on self-certification; (2) the certification requirement lacks force due to the U.S. government's weak enforcement practices; (3) there has been a persistent pattern of false claims of certification; and (4) U.S. companies have failed to adequately disclose their privacy policies, which precludes European consumers from determining the extent to which the companies adhere to the safe harbor principles.[12]

Although these concerns have been significant and persistent, they pale in comparison to the negative reaction in the EU following Edward Snowden's disclosure of the National Security Agency's bulk collection of data.[13] Since then, several EU data protection authorities have declared the safe harbor program "dead."[14] While others in the EU have been more measured — including Giovanni Buttarelli, the data protection supervisor for the EU — the EU consensus appears to be that the program should be shut down if significant changes are not made.[15]

The European Commission has made 13 demands aimed at addressing the lack of transparency, insufficient options for redress, lack of enforcement and access by U.S. authorities.[16] These demands include the following: (1) ex oficio investigations of companies to ensure compliance; (2) follow-up investigations of companies that have been found to be noncompliant; (3) notification of competent EU data protection authorities of doubts about a company's compliance; (4) investigation of false claims of adherence; (5) identification of national security exceptions and use of such exceptions only to the extent that they are strictly necessary or proportionate; (6) public disclosure of privacy policies; (7) a requirement that U.S. companies confirm status of compliance with the safe harbor program by including a link to the Department of Commerce's safe harbor certification website within their privacy policies; (8) publication by companies of privacy conditions of subcontractors; (9) publication by the Department of Commerce of all companies that are not currently in compliance with the program; and (10) provision of affordable and readily available alternative dispute resolution.[17]

The EU has threatened suspension of the program if its demands are not met, and has demanded results by the end of May 2015.[18] Due to the vested interest of U.S. businesses in the program, the U.S. has been scrambling to assuage the EU's concerns. Julie Brill, a FTC commissioner, has been touting the program as the "solution, not the problem" because it allows U.S. businesses and law enforcement to protect the data of EU citizens.[19] Both the Department of Commerce (with a focus on transparency) and FTC (with a focus on enforcement) have made efforts to address the EU's concerns.[20] As a result, U.S. companies that transfer personal data from the EU to the U.S. should expect that most of the EU demands will soon become requirements under the safe harbor program.

Expansion of the Right to be Forgotten

The "right to be forgotten" is certain to have an important role within the new EU data privacy regime. In *Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez* (C-131/12) (May 13, 2014), the European Court of Justice

(ECJ) established a "digital 'right to be forgotten'" that requires search engines to "remove links to web pages that are published by third parties and contain information relating to a person from the list of results displayed following a search made on the basis of that person's name."[21]

If Google's experience with the right to be forgotten is a guide, the expansion of this right will impose large costs on U.S. businesses with operations in Europe. Google had to create an internal apparatus to deal with all the requests that the ruling generated, and, in the year since the case was decided, Google has received more than 900,000 requests to be removed from search results. Google has had to decide each request on a case-by-case basis and develop criteria for assessing the requests.[22] Moreover, it has recently been reported that massive fines may be imposed for failure to comply with the law.[23]

Although ECJ's ruling in the *Costeja* case focused on "search engines," commentators immediately concluded that it was not limited only to search engines.[24] Nonetheless, it is not yet clear as to which companies the "obligation" to forget will be expanded besides other search engines. In determining that Google's activity was subject to the Data Protection Directive, the ECJ focused on a search engine's finding personal data "published or placed on the Internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to Internet users according to a particular order of preference."[25] This language is arguably limited to the specific activities of search engines but, read more expansively, may be construed as "umbrella" language that covers the activities of many different companies that handle personal data. Several commentators, therefore, anticipate that at least Twitter Inc. and Facebook Inc. will also be subject to the right to be forgotten.[26] Additionally, the anticipated expansion of the "right to be forgotten" as a result of reforms to the EU's data privacy laws may ensnare additional companies that handle personal data.[27]

Microsoft Warrant Case Fuels European Competitors

Microsoft's briefing of its appeal in *In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp.*, No. 14-2985-cv (2nd Cir.), begins with a harrowing hypothetical of the German Stadtpolizei seizing a *New York Times* reporter's private letters stored in a New York branch of Deutsche Bank AG through a warrant served on Deutsche Bank's German headquarters. Microsoft anticipates that such a seizure of private information would infuriate the U.S., which would see it as a violation of international and U.S. domestic law.[28]

Microsoft contends that the warrant at issue presents the real-life, digital version of that hypothetical, except that the "bad" actors are on the U.S. side, and are giving the Stored Communications Act an overly broad, unjustified application. In brief, the U.S. government applied for a "search and seizure warrant" targeting a specific @msn.com email account provided by Microsoft, and used by a person who is the subject of a government narcotics investigation. A federal magistrate judge issued the warrant, after which Microsoft undertook to locate the data associated with the account. Microsoft determined that this user's email "content" (the substance of the emails and their subject line) was stored at a data center operated by a Microsoft subsidiary in Dublin, Ireland. Microsoft did not produce this information and instead moved to quash the warrant on the basis that the SCA did not give extraterritorial power to search and seizure warrants. U.S. District Court Judge Loretta A. Preska rejected this argument and found Microsoft in contempt for failure to comply with the warrant.

In the appellate briefing to the Second Circuit, the parties and the numerous notable amici (including the Republic of Ireland, a Member of the European Parliament, privacy groups and prominent U.S. corporations) have confronted the scope and meaning of the SCA and the warrants issued pursuant thereto. Although Microsoft's appeal is likely to turn on those issues, the Second Circuit's analysis may also resolve whether an interpretation of the SCA that permits extraterritorial application of a warrant issued by a U.S. court conflicts with European data protection laws, thereby giving rise to legitimate comity concerns.

According to Microsoft and certain amici, the international reaction to the warrant decision is evidence enough of the conflict of laws and comity concerns. Microsoft trumpeted headlines from foreign newspapers, including one declaring "US Wants to Rule over All Servers Globally" and conveyed statements from the European Commissioner of Justice, who claimed the district court's order bypassed the established and proper procedures to attain such information.[29]

Additionally, Microsoft and certain amici argued that the ruling showed (on the U.S. government's behalf) further disregard for the privacy of information stored in Europe. For example, one amici, Jan Philipp Albrecht, is a member of the European Parliament and rapporteur for the draft legislation that will overhaul the EU data protection framework, including the requirements for transferring personal data to the United States.[30] Albrecht explains:

European citizens are highly sensitive to the differences between European and U.S. standards on data protection. Such concerns are frequently raised in relation to the

regulation of cross-border data flows and the mass processing of data by U.S. technology companies. The successful execution of the warrant at issue in this case would extend the scope of this anxiety to a sizeable majority of the data held in the world's data centers outside the U.S. (most of which are controlled by U.S. corporations) and would thus undermine the protections of the EU data protection regimes, even for data belonging to an EU citizen and stored in an EU country.[31]

These negative reactions are in the context of a push for Europe-based cloud computing services to replace U.S. companies to ensure that European data stays within Europe. According to Paul Nemitz, director of Fundamental Rights and Union Citizenship at the Directorate-General Justice of the European Commission, "'No German company that handles [its] data responsibly would trust an American cloud provider.'"[32] The warrant decision is also relevant to the pressing deadlines for proposals on U.S.-EU data transfers. The new EU data privacy framework is likely to tighten restrictions on exceptions for law enforcement and security agencies to access data stored in Europe.[33]

Given this context, even if the Second Circuit reverses the warrant decision, it may be too late. The warrant decision has already galvanized Europe to support the growth of a domestic cloud computing industry.

Endnotes

1 Brief for Member of European Parliament Jan Phillip Albrecht as Amicus Curiae at 6, *In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp*., No. 14-2985-cv (2nd Cir. Dec. 19, 2014), ECF No. 148.

2 Kara Swisher, White House. Red Chair. Obama Meets Swisher., Re/code, Feb. 15, 2015, http://recode.net/2015/02/15/white-house-red-chair-obama-meets-swisher/ (last visited May 14, 2015).

3 Jabeen Bhatti, Europe Faces 'Tough Choices' Regarding Data Privacy Regulation, EU Official Says, Bloomberg Law, May 4, 2015.

4 Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU at 2 (Nov. 27, 2013) (COM (2013) 847), http://feb.%2015,%202015,%20http//recode.net/2015/02/15/white-house-red-chair-obama-meets-swisher/ (last visited May 27, 2015) (hereinafter, Safe Harbor Communication).

[5] Federal Trade Commission, 2014 Privacy and Data Security Update, available at https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf(last visited May 13, 2015) (hereinafter, FTC 2014 Privacy and Data Security Update).

[6] U.S. Department of Commerce Safe Harbor Website, http://export.gov/safeharbor/ (last visited May 25, 2015).

[7] Safe Harbor Communication, supra note 4, at 4.

[8] Id. at 3 & n.6; Jabeen Bhatti, Commerce Official: U.S.-EU Safe Harbor Vital Because 'Huge Economic Interests at Stake', Bloomberg Law, May 4, 2015.

[9] FTC 2014 Privacy and Data Security Update, supra note 5.

[10] Safe Harbor Communication, supra note 4, at 4.

[11] Id. at 5.

[12] Id. at 6-8 (transparency); id. at 9-10, 13 (enforcement).

[13] Jabeen Bhatti, Multinationals Would Likely File Lawsuits If Germans Challenge U.S.-EU Safe Harbor, Bloomberg Law, March 31, 2015.

[14] Id.

[15] Bhatti, Multinationals Would Likely File Lawsuits If Germans Challenge U.S.-EU Safe Harbor, supra note 13; Bhatti, Commerce Official: U.S.-EU Safe Harbor Vital Because 'Huge Economic Interests at Stake', supra note 8.

[16] Safe Harbor Communication, supra note 4, at 18-19.

[17] Id.

[18] Karin Matussek, U.S. Data Talks Must Get Results by End-May, EU's Jourova Says, Bloomberg Business, April 13, 2015.

[19] Commissioner Julie Brill's Opening Panel Remarks European Institute Data Protection, Privacy and Security: Re-Establishing Trust Between Europe and the U.S. (Oct. 23, 2013), available at https://www.ftc.gov/sites/default/files/documents/public_statements/data-protection-privacy-security-re-establishing-trust-between-europe-united-states/131029europeaninstituteremarks.pdf (last visited May 27, 2015).

[20] Allison Grande, US-EU Safe Harbor Changes Coming Soon, Official Says, Law360, Dec. 3, 2014.

[21] The Right to Be Forgotten: Drawing the Line — Google grapples with the consequences of a controversial ruling on the boundary between privacy and free speech, The Economist, Oct. 4, 2014; Press Release No. 70/14, Judgment in case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, Court of Justice of the European Union, May 13, 2014.

[22] Jabeen Bhatti, EU Right to Be Forgotten Decision: One Year, Almost 1M Requests Later, Bloomberg Law, May 5, 2015.

[23] Julia Fioretti, Firms to face stiffer fines for breaking EU's 'right to be forgotten' rules, Reuters, May 20, 2015.

[24] See, e.g., Eduardo Ustaran, The wider effect of the 'right to be forgotten' case, Privacy & Data Protection Journals (Vol. 14, Issue 8) (Sept. 2014).

[25] Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez, Judgment of the Court, at pg. 23, ¶ 1 (European Court of Justice, May 13, 2014).

[26] Jeffrey Toobin, The Solace of Oblivion: In Europe, the right to be forgotten trumps the Internet, The New Yorker, Sept. 29, 2014; Lisa Fleisher and Sam Schechner, EU Regulators Take Aim at Google Search Privacy Conflicts: Expect to Name Subcommittee for Google Ruling, *The Wall Street Journal*, June 3, 2014.

[27] Elizabeth Dwoskin, EU Seeks to Tighten Data Privacy Laws, *The Wall Street Journal*, March 10, 2015.

[28] Brief for Appellant at 1-2, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985-cv (2nd Cir. Dec. 8, 2014), ECF Doc. 47.

[29] Id. at 13-14.

[30] Albrecht Amicus Curiae Br., supra note 1, at 3-4.

[31] Id. at 8.

[32] Jabeen Bhatti, U.S.-EU Safe Harbor Program 'Dead,' Two German State DPAs Proclaim, Bloomberg Law, Feb. 20, 2015.

[33] Matussek, supra note 18.