LOS ANGELES
Daily Journal
www.dailyjournal.com
WEDNESDAY, OCTOBER 21, 2015

Data privacy ruling will warp investigations

By Nathan J. Hochman and Martha B. Stolley

On Oct. 6, the European Court of Justice struck down a United States-European Union agreement that allowed companies to move personal electronic data between the EU and the U.S. In *Maximillian Schrems v. Data Protection Commissioner*, the ECJ deemed invalid a decision approving the so-called "safe harbor program" and said EU data protection authorities can investigate complaints about the transfer of personal data outside Europe. In addition, EU data protection authorities can suspend such data transfers until investigations are completed.

The safe harbor program was established following the European Commission's finding in 2000 that the U.S. has "inadequate" data protection laws. This would have been a severe restriction on the transfer of data to the U.S., so the European Commission and the U.S. Department of Commerce agreed on the safe harbor program to allow U.S. companies to transfer data from Europe provided they certify that they have abided by certain standards. The data transfer framework is enforced by the Federal Trade Commission. Over 4,000 organizations have current self-certifications of adherence to safe harbor principles.

New York Times

Max Schrems, plaintiff in the Schrems v. Data Protection Commissioner case, in Austria, Oct. 8.

Implications of Schrems

In *Schrems*, the ECJ said the approval of the safe harbor program was "invalid" because, among other reasons, U.S. "public authorities" are not subject to it. Thus, U.S. companies are "bound to disregard, without limitation" the program when instructed to do so by U.S. law enforcement. The ECJ also said the program does not provide EU citizens with adequate remedies to protect their data privacy rights in the U.S.

Schrems significantly expands the power of EU authorities to investigate suspected data breaches. Individual countries can now launch their own investigations, challenge the previously legal transfer of data pursuant to the safe harbor program, and, in some cases, suspend the transfer of data to the U.S. This could force U.S. companies to host user data exclusively within the EU country.

Internal Investigations

The ruling, which is final, will affect how U.S. companies investigate allegations of wrongdoing by affiliates in Europe, including Foreign Corrupt Practices Act investigations. A hallmark of any internal investigation into allegations of corruption overseas is the analysis of documents and communications originating within the country where corruption is alleged to have occurred. Many U.S. companies rely on the safe harbor to transfer data from the EU for analysis. Such companies either have safe harbor certification themselves, or they engage safe harbor-certified vendors. Now they must rethink this approach.

The primary legislation governing data protection in the EU — including the export of data — is Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. The directive protects "personal data," broadly defined as "any information relating to an identified or identifiable natural person." Thus, data generated solely for purposes related to an employee's work can still be deemed "personal" and cannot be transferred to countries with "inadequate" data protection laws, which includes the U.S. The need to abide by these EU data privacy laws absent the safe harbor program is in tension with the very real risk that U.S. law enforcement will punish a company for failing to sufficiently investigate possible FCPA violations.

Indeed, Assistant Attorney General Leslie R. Caldwell recently said the FCPA requires businesses that "tend to be exposed to corruption" to employ internal controls that include an "effective process … for investigating and documenting allegations of violations." Investigations into such allegations often require review of data from overseas. For reasons of logistics, cost and security, U.S. companies often seek to import such data to review. Now, depending on how regulators in Europe choose to employ the ruling, U.S. companies may be forced to conduct data processing and review in Europe. If particular national regulators agree with the ECJ that it is impossible for transferred data to receive EU levels of protection because of U.S. domestic law, then employees whose data is sought may successfully appeal to those regulators to block the transfer.

U.S. companies may also face difficulties responding to requests for information from U.S. authorities investigating their EU operations. Caldwell recently highlighted the need for U.S. companies to "ensure compliance with the laws of all the countries in which they operate." Yet, in the same remarks, she also said the Department of Justice will "challenge what we perceive to be unfounded reliance" on certain "foreign data privacy laws" to which corporations traditionally cite in their objections to document demands.

At the outset, the ECJ's invalidation of the safe harbor program should provide a legitimate objection to demands for EU data. The legitimacy of that objection will likely depend on the information sought, the individual EU nation in which the data is housed, and the extent to which national data privacy regulators exercise their powers to block data transfers.

Now What?

Prior data transfers under the safe harbor program were lawful, but it is unclear whether companies may continue to process such data. Furthermore, any new data transfer under safe harbor lacks a legal basis from the ECJ's perspective and could expose a company to liability.

Nevertheless, there are other methods that companies can use to transfer data, including securing free and informed consent to the transfer from the individual or from the local data protection agency. Consent from the former may be problematic in the case of the transfer of employee data, since consent must be explicit and freely given. In many European countries, you cannot rely on consent from employees because they are often considered not to have freedom of choice when that consent is provided. Given the discretion generally required in internal FCPA investigations, neither of these options is preferable or even feasible. The company likely will not want to disclose the possibility of internal corruption to local regulators, nor will it want to alert a suspect employee to the internal investigation and risk that the employee will destroy data.

Another option is for the entity receiving the data to enter either into a special standard data privacy agreement that has been approved by the European Commission or binding corporate rules (which allow a group company structure to transfer personal data to group entities internationally) that are pre-approved by one or more applicable data protection agencies. Still, there is a risk that the ruling could affect these options as well. In addition, some of the prior "adequacy" findings of the European Commission with other countries are now put into question.

The key permitted derogation under the directive that can allow for personal data to be transferred to the U.S. and other non-European countries is where such transfer is "necessary" to allow the organization to defend against or establish its legal rights. Typically, in the context of U.S. regulatory investigations, this exception is construed narrowly, and there is a need to conduct a form of review of personal data within Europe before the "necessary" information containing personal data is transferred to the U.S. for further investigation and possible disclosure to U.S. authorities. Furthermore, in some EU jurisdictions, the data protection agency must be notified before the transfer can take place, and there are further legal restrictions on the amount of personal data that can be transferred, as well as how the data must be protected.

While negotiators from the U.S. and the EU have sought to develop a new safe harbor program, U.S. companies must adapt immediately to the ruling or get caught in the rough and hostile waters of EU data privacy protection.

Nathan J. Hochman *is the deputy chair of Morgan Lewis & Bockius LLP's White Collar Litigation and Government Investigations practice group and a former U.S. Department of Justice assistant attorney general.* **Martha B. Stolley** *is a partner in Morgan Lewis & Bockius LLP's White Collar Litigation and Government Investigations practice group and a former Manhattan Assistant District Attorney.*