LJN LAW JOURNAL NEWSLETTERS

Cybersecurity

LAW & STRATEGY®

An ALM Publication

Volume 31, Number 2 • May 2016

International Cybersecurity Compliance Concerns

By Steven Rubin and Stephen Milne

Compared with the rest of the world, the United States has historically been a more open framework when dealing with information. Social media has made even the most mundane and possibly personal pieces of data available to many with a press of a finger. Such an open relinquishment of private information is almost assumed, and has become part of the American culture. Those who think about how easy it is to access data understand how their own data has become part of the searchable cyberspace.

The European culture and laws are different. Privacy rights are assumed, information confidentiality is maintained, and the concept of the United States "discovery" is scorned. There is a concern that European sensitive data should stay outside of the United States due to the protection of such data in the country not being sufficiently strong. It is therefore not a surprise that the laws in the United States and in Europe are inconsistent when it comes to cybersecurity.

Cybersecurity Law In the United States

The most significant piece of federal legislation in this area is the Cybersecurity Information Sharing Act (CISA), passed in December 2015. The purpose of this Act, purportedly, is to promote information sharing between the government and the private sector for issues relating to cybersecurity and new threat vectors. The idea is that sometimes industry is aware of new viruses or technical threats, but does not share the information with the government so that the government may protect itself and/or inform the public. CISA creates a voluntary means for companies to share their threat data with the government.

There are problems with sharing this information. While the act of sharing appears to be protected by statute, the underlying problem may not be. If I see a threat to my system, I could tell the government about that threat, and the act of telling would not create a new cause of action. But the law is not clear as to whether that sharing could then lead to a lawsuit relating to the *cause* of the sharing. Stated another way, I can tell the government I have a virus, and telling the government should not itself expose my company to liability. But I could later get sued for failing to comply with certain cybersecurity requirements because my system was infected with a virus and I did not take proper steps to protect the data.

So, trying to comply with United States laws alone creates a dilemma. But if you consider complying with CISA, you may also expose yourself to legal issues in Europe.

European Laws on Cybersecurity

Disclosure of personal data (capable of being used to identify a living person either on its own, or in conjunction with other data in the possession of the person controlling how the data is used) that relates to EU nationals could cause serious potential issues in light of recent developments overseas. Previously (before January 2016), many organizations relied upon the approved " Safe Harbor" regime framework developed by the Department of Commerce (DOC) in

Steven Rubin is a partner with Moritt Hock & Hamroff LLP in New York. **Stephen Milne** is a consultant with Memery Crystal LLP in London.

the United States and the European Commission, under which organizations could self-certify that they adhered to its principles. The certifying company gave binding promises that they complied with privacy policy requirements and provided protections for personal data which were sufficiently high that transfers of personal data from the EU to the United States would be permissible under the applicable Data Protection Directive (the Directive).

However, the Safe Harbor regime has suffered a huge blow by virtue of a recent decision in the Court of Justice of the European Union (CJEU). Maximillian Schrems was an Austrian citizen who had been a Facebook user since 2008. Facebook habitually transferred some data provided by its EU-based subscribers from its Irish subsidiary to servers located in the United States. Mr. Schrems lodged a complaint with the relevant supervisory authority in Ireland on the basis that the law and practice in the United States did not provide sufficient protection in relation to his data.

Initially, Mr. Schrems' complaint was rejected, particularly on the basis that the Safe Harbor regime ensured sufficient protection. However, on referral to the CJEU, the court held that the powers available to national supervisory authorities cannot be eliminated just because the European Commission originally decided that the Safe Harbor scheme provided such protection. The authority must look at the situation independently and determine whether the transfer of a person's data to a third country complies with the requirements of the Directive.

The CJEU then proceeded to consider the fact that public authorities in the United States are not subject to the Safe Harbor scheme. Further, national security, law enforcement and public interest all may prevail to the extent that a United States entity holding or processing data may be forced to ignore the requirements of the Safe Harbor scheme where it conflicts with any of the foregoing. As a result, data would not be protected in such circumstances and there were no clear limitations or restrictions on the public authorities' abilities.

In addition, there was no clear ability for individuals to pursue legal remedies in order to access their data or to have it rectified or erased, which the CJEU viewed as inherent in the existence of the rule of law and as compromising "the essence of the fundamental right to effective judicial protection." The CJEU therefore held that the original European Commission decision that Safe Harbor privacy principles provided adequate protection was invalid — effectively nullifying the Safe Harbor option.

What Now?

The Safe Harbor route is no longer a valid basis upon which personal data can be transferred from the European Union to the United States. But there is not, as of yet, clear guidance as to what will replace it. Indeed, different data protection authorities (DPAs) have been taking different approaches to this evolving situation.

For example, the Information Commissioner's Office (ICO; the supervisory data protection authority for the United Kingdom) has been advocating that continued use of the Safe Harbor principles may still be a sensible proposition in the interim. The ICO further indicated it will not take enforcement procedures yet, until an approved alternative to Safe Harbor has been determined. However, this guidance is not legally binding and the ICO is posed to reiterate that companies need to review their compliance processes and procedures.

This approach has been somewhat reflected in guidance from the Spanish regulator, which has indicated that it will not rush to take enforcement action against companies provided they are working on appropriate proposals and arrangements to ensure adequate protection of personal data. However, in stark contrast, the data protection authority in Hamburg, Germany, has already made it public that it does not expect organizations to continue relying upon Safe Harbor and that it will take immediate enforcement proceedings against any that do continue to transfer personal data outside the EU in this way. Such proceedings could lead to fines up to €300,000 (roughly $340,000) per data breach.

Some Proposed European Solutions

The Article 29 Working Party (which is made up of representatives from the data protection authorities of the EU states) recently confirmed that it views use of binding corporate rules and model contract clauses as valid options to enable the transfer of data from the EU to the United States.

Binding Corporate Rules are essentially rules operated by an organization that put in place adequate safeguards for protecting personal data in line with the Article 29 Working Party's requirements. They are not, however, a quick fix — as such rules require an application to, and approval from, the relevant data protection authority via a relatively cumbersome design and implementation procedure that usually takes in the region of 12-18 months.

Model contract clauses are, on the other hand, considerably easier to implement provided both parties are in agreement. These provide for an approved set of contractual obligations that eliminate the requirement for the transferee of data to make their own assessment regarding the adequacy of the protections provided. There are different sets of clauses depending upon the parties' relationship and what they do with the data.

A further possibility is to obtain express consent to the transfer of the data. However, even the more relaxed data protection authorities are closely scrutinizing this route to effecting transfers, as the key concern is whether consent is specific enough for what is happening to the data and whether it provides any real protection to the individual. Much has been made in recent months of high-profile examples of data having been harvested from individuals on the back of a generic data consent, and having then been retransferred, reused and resold multiple times in manners the individual who gave "consent" could not possibly have anticipated. Consent on its own may well not be enough.

Privacy Shield

The European Commission and the DOC have agreed upon a new arrangement, known as the "Privacy Shield," as a replacement for the now defunct Safe Harbor scheme. The Privacy Shield is in fact a collection of principles, including:

1. Choice — individuals will have the ability to opt-in or out as far as sensitive data is concerned, as regards third-party marketing and in relation to any new use of their data that was not initially contemplated.

2. Notice — individuals must be informed of their rights, the principles of Privacy Shield and given a contact for complaints. They must also be given details of sharing and disclosure of their data (including public authorities), and organizations will have to confirm their liability for data processing.

3. Accountability — organizations will be required to put in place formal contract arrangements in writing for onward transfers of data to other controllers or processors (with only limited exceptions).

4. Security — security measures must be implemented that are reasonable based on the nature of the processing and the personal data being processed.

5. Integrity and Limitation — data will have to be kept up to date and accurate, and data collection will have to be limited strictly to what is relevant in the circumstances.

6. Access — individuals will have the right to access their data and to require its correction and/or deletion (unless the cost of doing so would be overly burdensome).

7. Recourse/enforcement — this is one of the crucial proposals. It provides for a free means of recourse for individuals to be provided by the organization with the ability for individuals to escalate complaints to local data protection authorities if the issue is not satisfactorily dealt with. If that does not resolve the matter, then there is even scope for individuals to potentially initiate arbitration claims.

Privacy Shield is still a little way off, however, as intended implementation was set for June 2016, but there are still a number of criticisms leveled at it by both politicians and commentators and implementation has been delayed. In addition, the General Data Protection Regulations are upcoming (albeit not until April 2018) and these will bolster both the EU's data protection authorities' powers and their likelihood to crack down on enforcement.

Conclusion

Each organization needs to review its current compliance arrangements and re-evaluate on the basis of the above issues, implementing sensible interim solutions, at least, to avoid falling foul of the more aggressive data protection authorities and their willingness to impose potentially sizeable fines.

—❖—