Client Alert.

16 December 2010

The Butterfly Effect: Outsourcing, the USA PATRIOT Act and OFAC

By Alistair Maughan, Oliver I. Ireland and Panagiotis C. Bayz

As a demonstration of the butterfly effect of chaos theory, changes made to U.S. law after the 9/11 terror attacks are now being raised as blockages on the competitiveness of U.S.-based outsourcing and IT services companies when competing for business in Europe and Asia.

The USA PATRIOT Act contains provisions allowing the U.S. government access to business records for foreign intelligence and international terrorism investigations. The extraterritorial effect of the USA PATRIOT Act means that confidential data of non-U.S. outsourcing customers is potentially open to disclosure to the U.S. authorities via any U.S.-based service provider (or its non-U.S.-based affiliate) handling that data.

This Client Alert examines the effect of the USA PATRIOT Act – and the extraterritorial effect of the U.S. Office of Foreign Assets Control rules – on non-U.S. entities that enter into outsourcing or IT services arrangements with U.S. corporations or their overseas subsidiaries. In particular, it addresses whether a non-U.S. subsidiary or affiliate of a U.S. corporation may be required under the USA PATRIOT Act to disclose to the FBI data belonging to its customers, and what actions non-U.S.-based customers can take to retain control of their data.

THE USA PATRIOT ACT

Section 215 of the USA PATRIOT Act, enacted in the months following the 9/11 terror attacks, provides the U.S. government with the means to access to business records for foreign intelligence and international terrorism investigations.

Specifically, section 215 of the USA PATRIOT Act permits the FBI to apply for an order "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." If a U.S. judge finds that an FBI application meets the relevant requirements, the judge must enter an *ex parte* order approving the release of items sought.

The USA PATRIOT Act is extraterritorial in application: it permits the U.S. authorities to enforce its provisions against non-U.S. entities and non-U.S. data. The extraterritoriality applies via corporate ownership and the location of servers or data. It would not be a defense for a U.S. company which possesses or processes data to say that it does so outside the U.S. It would be harder, but by no means impossible, for the U.S. authorities to enforce disclosure provisions on a non-U.S. entity with operations overseas. The position of a non-U.S. affiliate of a U.S. parent which processes data outside the U.S. is less clear: much would depend on the degree of connection to the U.S.

If the recipient of a section 215 order is, for example, an EU-based entity and the entity chooses to disregard the court order, a judge may attempt to enforce such order against the U.S. parent of the EU-based entity. In addition, the U.S.

parent itself may be direct recipient of the section 215 order. These circumstances present a different scenario because the U.S. parent corporation would be within the jurisdiction of the judge that issued the section 215 order. The U.S. parent corporation would need to decide whether to challenge or comply with the order. As a result, whether or not the order would cause the production of the EU-derived information would likely depend on the U.S. parent corporation's control over the EU-based entity and the U.S. company's willingness to challenge the U.S. government in order to protect its customer.

Under both scenarios, the U.S. parent corporation may request that the EU-based entity disclose the EU-derived information to the FBI. But, if the U.S. parent corporation did not have sufficient control over the EU-based entity, the U.S. parent corporation could not require the EU-based entity to produce the information. In other words, unless the EU-based entity was controlled by its U.S. parent corporation, the EU-based entity would have the option to refuse to produce EU-derived information to the FBI.

In this context, the USA PATRIOT Act does not set out a clear definition of control that would govern whether the U.S. parent corporation controlled the EU-based entity and could require it to produce information. This determination is likely to be highly fact-dependent. Further, to the extent that a U.S. parent corporation sought to isolate a company from its control for purposes of performing a contract with that EU-based customer, the U.S. corporation would lose the ability to control the quality of the services provided. Nonetheless, it should be possible for a U.S. parent corporation to retain a significant economic interest in an EU-based entity, such as through the ownership of non-voting preferred stock, without having the actual ability to control the actions of the EU-based entity.

EFFECT ON OUTSOURCING AND IT SERVICES

In some situations, section 215 of the USA PATRIOT Act can have a significant potential effect on outsourcing and IT services contracts.

For example, assume that a European bank wishes to outsource services which involve access to, or processing of, its European customers' data. The bank chooses as its service provider a well-known and highly reputable global but U.S.-headquartered service provider. The bank will no doubt include in its contract robust privacy and data security arrangements, including provisions that comply with EU data privacy laws which prohibit transfers of data outside the European Economic Area. The bank may think that there is no chance of its data being disclosed to the U.S. government (or, indeed, anyone else) without its consent. It would be wrong.

- If the bank has contracted directly with a U.S.-based company, the service provider is clearly subject to the jurisdiction of U.S. authorities. When faced with a choice between its contract with its customer and the combined might of the FBI and the U.S. government, there must clearly be a possibility that the service provider would disclose any information demanded by U.S. authorities.
- Anti-tip-off provisions in the USA PATRIOT Act prevent the service provider from informing its customer of the order for disclosure.
- The customer may include contractual provisions requiring the service provider to resist or challenge any subpoena under the USA PATRIOT Act – but how far must the service provider go to comply with such provisions?
- Even if the bank has been careful to enter into a contract with a non-U.S.-based subsidiary or affiliate of the U.S. parent and to ensure that the service provider doesn't use any U.S.-based resources to undertake services under the contract, it is not necessarily exempt. The USA PATRIOT Act has extraterritorial effect, and the FBI and U.S. Department of Justice can seek enforcement against non-U.S. subsidiaries of U.S. corporations.

POSSIBLE PROTECTIONS AND THEIR LIMITATIONS

The U.S. authorities may only seek disclosure or data if the items sought can be obtained with a *subpoena duces tecum* issued by a court of the United States in a grand jury investigation or with any other order issued by a U.S. court directing the production of records or tangible things.

The U.S. Department of Justice ("DOJ"), which generally represents the U.S. in legal matters, has issued guidance relating to the government's abilities and limitations with respect to *subpoena duces tecum*. Specifically, the Antitrust Division Grand Jury Practice Manual ("DOJ Manual") provides guidance, based on relevant U.S. case law and the DOJ's broad practical experience, for all DOJ personnel with respect to the performance of their grand jury-related responsibilities. The DOJ Manual clarifies, for example, that a *subpoena duces tecum*:

a. may be served on any legal entity or corporation, including foreign affiliates of U.S. companies;

b. may not be served on a foreign government;

c. may seek any type of non-privileged document or physical evidence; and

d. must be reasonable in scope.

Section 215 provides no scope or guidance relating to the jurisdiction of a U.S. judge to issue an order to foreign entities. Because section 215 provides no limitations on the types of persons to whom a judge in the U.S. may issue an order, a judge would have the authority to issue such an order to a non-U.S. entity that is a subsidiary or affiliate of a U.S. corporation or to the U.S. corporation itself. A judge may choose not to issue such an order on grounds of comity, although we are not aware of any instances where a judge has refused to do so – but it is possible that this could happen especially if the information at issue belonged, say, to a foreign government entity as opposed to a bank or company.

The DOJ Manual also recognizes that subpoena recipients may be prevented from complying with the requirement to produce documents by virtue of local country "blocking statutes" which render the provision of the material unlawful under local law where the information or its holder is based. Unfortunately, the DOJ Manual does not specify what form a blocking statute might take nor set out a definitive list of existing statutes. It does, however, mention Germany, Australia, France and the U.K. as examples of countries that potentially possess a blocking statute.

Therefore, a non-U.S.-based outsourcing customer may take some comfort in the fact that even the DOJ recognizes that local laws may limit the extraterritorial jurisdiction of the USA PATRIOT Act. The problem remains, however, that much will depend on the attitude of the U.S. service provider or its overseas affiliate that gets served with the order to produce documents or data.

For a start, the USA PATRIOT Act contains anti-tip-off provisions, so the service provider would be in breach of U.S. law if it were to tell the customer about the subpoena, its scope or its proposed response.

Also, the customer can't be sure which way the services provider will proceed when faced with legal action by the U.S. authorities. Will it stand behind its customer, cite the contract provisions on confidentiality and data privacy, and enforce the local "blocking statute"? Will it take steps to challenge the subpoena through the U.S. courts, and how far must it go (and how much must it spend) to do so? Or will it decide that, at the end of the day, its loyalties and long-term commercial interests lie in cooperating with the U.S. authorities?

PRACTICAL GUIDANCE

Non-U.S.-based outsourcing customers can take steps to minimize the likelihood of their data being subject to orders of production under the USA PATRIOT Act.

First, if confidentiality of data is a major concern it is clearly better to contract with a non-U.S. subsidiary than with the U.S. parent – although there may, of course, be a number of offsetting reasons (including maintaining financial stability) why one might prefer a direct parent company contract.

Second, if you do contract with a non-U.S. subsidiary, you should check the organizational structure of a service provider to ensure that data is only held by non-U.S. companies that are clearly not subject to significant levels of U.S. management, share ownership and control. You should probably back this up with contractual requirements which prevent changes to organizational structure without customer consent.

Third, contracts should go as far as is permissible to require service providers to notify and consult with the customer prior to any legal request for enforced disclosure of documents or data. Contracts should also deal with the issue of the service provider's obligations to challenge any order or subpoena through the U.S. courts.

Finally, contracts should expressly tee up the blocking statute defense, *i.e.*, state that disclosure under the USA PATRIOT Act is expressly prohibited and a violation of the local data protection or privacy statute. Customers may go further and elevate disclosure to foreign government authorities to the status of a terminable event, or at the very least, require service providers to indemnify their customers from any third party claims that are asserted (*e.g.*, from affected individuals) as a result of the disclosure.

AND ANOTHER THING … THE OFAC RULES

In fact, the provisions of section 215 of the USA PATRIOT Act are comparable to another set of U.S. laws that have a similar effect.

Under the trade sanctions and economic embargoes administered by the Office of Foreign Assets Control ("OFAC"), a part of the U.S. Treasury Department, U.S. persons may not engage in trade, financial transactions and other dealings with certain designated countries or with a person or entity identified on the list of Specially Designated Nationals and Blocked Persons ("SDN"). In order to comply with the OFAC rules, U.S. companies screen transaction counterparties against the SDN list. If there is a match with the SDN list, the U.S. company is obliged to cease doing business with that person. Financial institutions are obliged to give notice to OFAC of a positive match. However, when even non-financial sector companies believe that they may have engaged in a transaction with a person on the OFAC SDN list, they often elect to disclose such violation voluntarily to mitigate potential penalties.

The effect of the OFAC rules on outsourcing by non-U.S. companies differs according to circumstances and the approach taken by service providers. There have been cases where U.S.-based service providers to high-profile European outsourcing customers have taken "doing business" literally and have cross-checked the SDN list in relation to all customer data processed.

Take the example of a U.S. company that wins the contract to process citizens' data held by a large European government agency. The view here could be that the OFAC regulations require the U.S.-based company to verify that it is not doing business directly or indirectly with individuals on the SDN list, and so it is at significant risk of civil or criminal penalties if, in the course of performing services, it processes data relating to an OFAC prohibited person; and the only

way of managing this risk is for the U.S.-based company to check each name against the SDN list.

The customer in this example would clearly consider that the matching of names against the SDN list is in breach of the services agreement, and that use of data is not authorized under local law, thus creating potential liability for the customer (as "data controller") to citizens whose data are so processed as well as potentially violating local data protection law.

The customer would equally object that the OFAC cross-checking requirement does not apply here because the U.S. company is not providing any services direct to citizens (*i.e.*, the contract is with the government agency). However, the scope of the OFAC regulations also prohibits U.S. persons from "facilitating" (which is defined broadly in the regulations) transactions with an SDN. If the customer's client is an SDN, OFAC would take the view that the U.S. person is facilitating a transaction with an SDN, and thus engaged in an OFAC-prohibited transaction.

CONCLUSION

Outsourcing contracts between non-U.S. customers and U.S. service providers (or subsidiaries of U.S. service providers) should be adapted to address the issues that arise under the USA PATRIOT Act and the OFAC rules. Customers should take into account any additional risks to the security and confidentiality of their data when selecting a service provider, and may need to take structural or contractual steps to maintain data security for their, and their customers', protection.

Contact:

Alistair Maughan
+44 207 920 4066
amaughan@mofo.com

Oliver I. Ireland
(202) 778-1614
oireland@mofo.com

Panagiotis C. Bayz
(202) 887-8796
akibayz@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for seven straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.