Looking outside the Prism: how safe are data transfers?

Gail Crawford and Fiona Maclean, from Latham & Watkins, consider the current methods of data transfer outside the EEA and the extent to which they permit disclosure by the recipient entity to law enforcement, discuss what the future may hold under the proposed Data Protection Regulation, and explain what steps organisations can take to manage the risk of the conflicting legal regimes

When former NSA contractor, Edward Snowden, leaked documents disclosing the NSA's mass surveillance programme, known as PRISM, he re-invigorated the debate on, and the media interest in, the validity of the current safeguards for trans-border data flows from the European Economic Area ('EEA'). Following the European outrage at the PRISM scandal, European authorities, activist groups and individuals are left questioning the safety of data of European citizens once outside of the EEA. Recent statements by the European Union Justice Commissioner, Viviane Reding, and the recent vote by the European Parliament's Civil Liberties, Justice and Home Affairs ('LIBE') Committee prove that this is a very unsettled area of the law.

Methods of data transfer outside the EEA

The vast majority of large global businesses use the European Commission's standard contractual clauses, commonly known as the 'Model Clauses', for the transfer of personal data to third countries or, in relation to transfers to US companies that are members of the US Safe Harbor programme, rely on that company's Safe Harbor certification. Companies can also gain approval for data exports within their group by obtaining approval of Binding Corporate Rules ('BCRs'), although, as these have to be approved by their local data protection authority, the uptake has been reasonably low. Furthermore, the European Commission has determined that some third countries ensure an adequate level of protection for personal data and, so, transfers to countries on the Commission's approved list can be undertaken by following the same procedures as for transfers to countries within the EEA.

Safe Harbor

Safe Harbor is based on seven basic principles: Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement. Members self-certify with the US Department of Commerce that they will comply with these principles. US Safe Harbor has been challenged in Europe in recent years, with European countries, particularly Germany, criticising it for its lack of rigour given it relies on self-certification (with no audit function to check compliance). This is emphasised by the US Federal Trade Commission enforcement actions against Myspace, Google and Facebook for deceptive practices, for example misleading customers by not complying with their self-certifications and privacy statements.

Recent criticisms in the wake of the PRISM scandal have focussed on whether derogations under the scheme, which allow members to deviate from the principles 'to the extent necessary to meet national security, public interest or law enforcement requirements', undermine the integrity of the Safe Harbor principles and have led Viviane Reding, in July 2013, to state that "The 'Safe Harbor' agreement may not be so safe after all".

In its open letter to Ms Reding in August 2013, the Article 29 Working Party questioned how this exception to adherence to the principles, when applied by the US authorities in the way suggested by the PRISM disclosures, could be aligned with European data protection requirements. The nub of the issue is the divergent view as to what level of surveillance and access to data is 'necessary' for the NSA to protect the public interest. It is probably accurate to say that the United States and various EU countries differ in how they balance the rights of the individual with the wider aims of surveillance, with the EU taking a more protective stance over the individual, while the US arguably adopting a more government-friendly position. This disparity in approach may, in itself, be reason enough for the EU to revisit Safe Harbor.

Model Clauses

While Safe Harbor hits the spotlight, escaping (relatively unscathed) from the PRISM backlash are the Model Clauses. The Model Clauses are designed to facilitate the transfer of personal data from the EEA to third countries by imposing sufficient contractual safeguards for the privacy of

individuals. There are different forms of clauses for transfer to data processors (for example, service providers) and data controllers.

Whilst on the face of it the form for transfers to other controllers contains a prohibition on any disclosure to an overseas law enforcement agency (i.e. to a controller located in a third country) without the data exporter's consent, the text of the actual decision states that the clauses are 'subject to any mandatory requirements of national legislation which do not go beyond what is necessary in a democratic society, e.g. a necessary measure to safeguard national security, defence, public security or the prevention, investigation, detection and prosecution of criminal offences', which essentially means that controllers in a third country do not need to comply if, in doing so, they would breach local law.

The form for processors approved in 2010 does not include any express restriction on disclosure of data. While it imposes an obligation on the data importer to notify the data exporter about any legally binding requests received from a law enforcement authority, that requirement does not apply if the processor is legally prohibited from doing so.

The impact of this is that European companies can comply with the export rules by using the Model Clauses, yet the data importer can also disclose data to third parties where required to do so by local law, and the EU controller will not be informed of the disclosure where the request or order was sealed (as in the case of NSA orders).

Therefore, while public interest in the adequacy of the Model Clauses may not have been piqued to the same extent as it has in relation to the Safe Harbor scheme (presumably because of the US angle of PRISM), there are undoubtedly still questions that need to be answered.

Binding Corporate Rules

Support for BCRs has been strong in recent years, with the Article 29 Working Party issuing its 'Binding Safe Processor Rules' earlier this year and the new Data Protection Regulation expressly referring to BCRs as a method for transfer. However, the BCRs framework also does not solve the issues which have come to the fore following Snowden's disclosures.

The framework issued by the Article 29 Working Party on BCRs provides that organisations must have mechanisms in place for dealing with issues such as conflicts of law (for example, a request by a US authority for data held by a subsidiary in the EU), but does not provide guidance on what such mechanisms should be, other than that the regulator should be consulted in cases of doubt. Therefore, while organisations may attempt to ensure that they have BCRs which are fit for purpose and provide adequate protection for their data, very little direction is available on the exact steps that businesses should take.

> ***"Only collect data you need and delete data you do not — if you do not hold it, you cannot be required to disclose it. Having a retention policy which is based on actual requirements, rather than standard positions which have no correlation to real business needs, limits the organisation's exposure to data requests as well as security breaches."***

What does the future hold for data transfers under the draft Regulation?

Early drafts of the EU Data Protection Regulation, which were leaked to the public at the end of 2011, introduced a blocking provision setting out a strict process for dealing with law enforcement requests by foreign authorities, except where the provisions of any applicable mutual assistance treaty were followed (under which requests for data must be made via the agreed inter-governmental channels, effectively resulting in approval from the home country). The provision states that a controller must notify the applicable regulator without undue delay, and prior authorisation from the regulator must be obtained, before any transfer was permitted. By the time the official draft Data Protection Regulation was released on the 25th January 2012, these restrictions were conspicuous only by their absence.

In an interesting twist of fate, while it is believed that public interest and political attention (substantially from the US) around this provision led to its deletion prior to publication of the official draft, less than 12 months on, public interest and political attention surrounding PRISM has led to this requirement being reintroduced. The LIBE Committee, heavily influenced by the NSA revelations, voted to approve a compromise draft Regulation on 21st October 2013, reintroducing the requirement for consent from the applicable supervisory authority prior to any law enforcement disclosure. Under the proposed amendment, it would be necessary for important grounds of public interest, recognised in European Union law or the law of the country to which the controller is subject, to be established to gain consent.

Further amendments to the draft Regulation passed by the LIBE Committee include the reintroduction of the drop dead date two years after the Regulation takes effect, after which all decisions on adequacy, for example those approving the white list of countries with adequate data protection laws, the Model

(Continued on page 8)

(Continued from page 7)

Clauses and Safe Harbor would cease to have effect. This evidences the EU's perceived need to revisit data export in its entirety.

These proposals are a clear message from Europe in response to the PRISM scandal. However, as demonstrated by the first attempt at the introduction of such provisions (following the earlier leaked versions of the Regulation), it is unlikely that these amendments will be welcomed in the US. While commentary on the LIBE vote is still in its formative stages, the Federal Trade Commission's ('FTC') 'response' to the unofficial drafts of the Regulation in 2011 stated that it viewed blocking provisions of this nature as a backward step that would have an adverse effect on the global interoperability of privacy regimes and enforcement cooperation between the EU and the rest of the world. (These comments were made in an 'Informal Note' from the FTC, also leaked).

Whether this requirement for regulatory approval will again be eroded by inter-governmental lobbying as the Regulation continues through the legislative process, remains to be seen. The future of the Regulation is at best unclear, with both Germany and the UK supporting delay at the EU Heads of State summit at the end of October. So what does this uncertainty mean for businesses and their data transfers?

While the uncertainty surrounding the various mechanisms for transferring data outside of the EEA continues, organisations are left with no clear 'safe' option for ensuring that their data are not disclosed by service providers they use in third countries, or how to deal with the conflict between EU and US laws (for example, the fact that a US headquartered organisation can be required, under US law, to disclose data in stored in Europe even though such disclosure will breach the laws in the country in which it is held). Accordingly, businesses must ensure that they take other steps in structuring their data model in a manner that enables them to manage the risk of data being disclosed in response to governmental requests.

Understand your data

Do not assume that dealing with data requests by authorities is an issue specific to the US: Countries globally (including in the EU) frequently request data. It is therefore imperative to understand whether the data you hold are likely to be requested by law enforcement bodies, where such data are hosted/accessible (regardless of physical location) and where the entity that ultimately controls those operations is situated.

Carefully consider the use of service providers

Before disclosing any data to a service provider or group company outside the EEA, any risk assessment should take into account whether such transfer increases the risk of disclosure to government or administrative bodies and the impact of that (and any associated publicity) on your organisation. Consider whether it is wise to use non-EU service providers with caution and note that it is not sufficient that a service providers' operations are in the EU; if an EU provider has a non-EU parent it may still be required to disclose data from its EU operations. It is also important to understand how, in practice, the service provider will deal with the receipt of orders and requests. If terms and conditions are open for negotiation (often not an option with cloud providers and the like), ensuring that clear notification obligations are set out therein can help limit exposure.

Transparency

Another step that organisations may wish to consider is to ensure transparency of potential data disclosures and/or transfers in customer contracts. If you are not able to ensure that data will never be disclosed, do not over-promise the security of your data to your customers. Adopting an open and transparent approach with customers minimises the likelihood of challenge by customers who subsequently learn that their data are being transferred overseas.

Data minimisation and proportionality

Only collect data you need, and delete data you do not — if you do not hold it, you cannot be required to disclose it. Having a retention policy which is based on actual requirements, rather than standard positions which have no correlation to real business needs, limits the organisation's exposure to data requests as well as security breaches.

Is EU-US agreement the answer?

We maintain that this is, in essence, a political issue which needs to be solved at an inter-governmental level. The issue is similar (although broader in scope) to those we have seen before about the US government's access to airline passenger name records and the international banking data held by SWIFT. The solution finally reached in both these cases was an inter-governmental agreement imposing controls on the scope of data that could be accessed. However, until such an agreement is reached, organisations operating in the US and the EU remain at risk of being caught between a rock and a hard place as they weigh the potential disadvantages of either breaking EU data protection rules or US laws requiring disclosure of data.

Therefore, until progress is made on this highly charged political issue, the best that organisations can do is to ensure that they understand the risks in relation to the data they hold given their global data model and use of service providers. In the meantime, we watch with interest to see how this matter plays out on both sides of the Atlantic. The gauntlet has been thrown down by Snowden — whether the EU and the US will respond quickly with a sensible solution that provides clear guidance to industry, or will remain at odds, remains to be seen.

Gail Crawford and Fiona Maclean
Latham & Watkins
gail.crawford@lw.com
fiona.maclean@lw.com