Big data

Image: Jason Reed/Ryan McVay/iStock/Thinkstock

ZETTABYTES AND THE EMERGING REGULATORY RISKS

A NIGHTMARE ON SERVER STREET

Derek Patterson, **Yousr Khalil** and **Toby Duthie** of Forensic Risk Alliance take a look at what the advent of big data and always-on electronic communications means for corporate investigations.

Information technology and data in the new world

The world of information technology, from computers to "the Cloud", has fundamentally changed almost every aspect of our professional and personal lives. It has delivered amazing productivity benefits, although with these benefits come significant challenges and risks. Technology company EMC estimates that digital data volumes are doubling every year and by 2020 there will be almost 44 zettabytes in existence (one zettabyte equals one trillion gigabytes). Other staggering statistics which convey the speed at which data is being created each minute include:

- 4.11 million search queries for Google;
- 571 new websites launched;
- 31,000 new photos posted to Instagram; and
- 47,000 app downloads via Apple.

The staggering changes of "always-on" electronic communications and the proliferation of electronic documents and data sources have altered the IT environment completely. Statutory and legal responses have been uncoordinated and slow, and as a result corporations, particularly those with a global presence, are being tested with new and difficult challenges.

Emerging challenges and a changing environment

For the chief information officer and the board, the evolution and growth of challenges has been formidable. Initially these challenges were primarily budgetary (ie, the costs of the hardware and software versus productivity savings). To this were soon added architecture and effectiveness challenges – ensuring the overall IT system was well organised, functioned 24/7, supported the needs of the business and did not expose the business to failure risk.

But newer and more holistic risks are emerging for corporate IT teams, with regulatory risk and data vulnerability currently at the forefront. Now, more than ever before, corporate IT teams need to be interacting with their general counsel, compliance colleagues and external advisers, a requirement and skill set few would have thought necessary only a short while ago.

The well-publicised Edward Snowden affair was a wake-up call for the world on the vulnerability of data systems and the seemingly easy access US agencies have to private data. The US National Security Agency (NSA) secretly collected data stored on the servers of internet corporations such as Google, Yahoo! and Facebook. Between January and June 2013 (the period preceding the affair), Apple indicated that it received between 1,000 and 2,000 requests for data from the US government. Due to the existence of US government secrecy

First published in **Global Investigations Review** Volume 1 Issue 2

Big data

requirements, Apple and other companies cannot disclose to their customers how often and why their private data is disclosed to enforcement agencies.

Recently, one of the Snowden documents revealed surveillance activities carried out on behalf of the NSA on the communications between a US law firm – Mayer Brown, according to press reports – and its client, the government of Indonesia, which the firm was representing in trade negotiations involving the US government. According to the document, the NSA instructed its counterpart, the Australian Signals Directorate, to monitor these communications (which according to US law would have been deemed attorney-client communication).

Often, we have heard non-US corporations suggest that US-driven disclosure orders and subpoenas could be linked to or driven by US commercial interests. At face value, this Snowden document could potentially support this theory. It also highlights the extent to which the US is able to exert influence over its friends and allies.

The Snowden affair has also directly clouded political relationships between the US and countries or political figures that were subject to this surveillance – notably German chancellor Angela Merkel, French president François Hollande and Brazilian president Dilma Rousseff, all of whom have championed measures to limit this US-driven worldwide internet surveillance.

The German chancellor in particular is championing a European network to limit the transfer of personal data to the US, and possibly block US-based internet service providers. Practical implementation and data protection laws would potentially prevent this from happening, however.

Throughout the European Union (with perhaps the exception of the UK), there is also an increasing clamour to boost and harmonise the privacy laws. On 12 March, the European Parliament voted overwhelmingly in favour of new data protection laws. According to a press release:

> *MEPs inserted stronger safeguards for EU citizens' personal data that gets transferred to non-EU countries in a major overhaul of the EU's data protection laws… The new rules aim both to give people more control over their personal data and to make it easier for firms to work across borders, by ensuring that the same rules apply in all EU member states. MEPs also increased the fines to be imposed on firms that break the rules, to up to €100 million or 5% of global turnover.*

If implemented and enforced, this would be a game changer for multinational companies. However, implementation and consistency across Europe remain difficult, and present a complex and ever-changing landscape for corporations to navigate through.

In a similar vein, Brazil's President Rousseff was successful in enacting legislation for protection of data. In March, Brazil's lower chamber of congress approved its "anti-spy" internet legislation, which requires internet companies to comply with local Brazilian laws in cases involving information on Brazilians, regardless of the location of the data. Earlier versions of the legislation called for companies to establish and maintain data on Brazilian servers inside the country. Given the considerable cost associated with this requirement, it was later dropped in favour of approving the overall bill.

Safe harbours – the present, the future and the e-discovery myth

The safe harbour agreements between the US, EU and Swiss organisations were created to facilitate the cross-border transfer of personal data in the context of everyday business without violating relevant European data privacy laws. The framework and related certifications have been criticised by a number of individuals and organisations, including within the European Commission, which has resulted in a loss of trust in its effectiveness. The framework as it currently stands requires a straightforward self-certification process with no independent proof of compliance. Furthermore, the framework covers data transfer for the purpose of storing customer information, but, as it is primarily designed to assist in non-contentious everyday business, it does not address other data processing requirements under e-discovery processes or respond to US discovery by enforcement agencies or civil plaintiffs.

The EU is assessing potential changes to strengthen the current safe harbour framework and allow for potential financial recovery from US corporations in breach of the framework's requirements via legal claims brought forth in EU – and not US – courts. In addition, the proposed changes include amendments requiring organisations to "implement technical and organisational measures" that are "appropriate to the state of the art and the risks represented by the processing of the nature of the data processed" instead of only taking "reasonable precautions".

Whatever the outcome of this, the framework and proposed amendments continue to exclude the collection and exchange of data when responding to cross-border criminal investigation and litigation. Under the existing regulations, members are required to obtain "explicit (opt in) choice... if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorised subsequently by the individual." The framework does not address what notifications and approvals are required when responding to regulatory investigations exposing the companies and individuals collecting the data to significant risks during a criminal evidence-gathering process. Given the current post-Snowden climate, these risks would appear to be growing significantly.

Risk management in the litigation and regulatory investigation context

Compliance with regulatory laws regarding data privacy and blocking statutes, and managing the risk of data vulnerability, is a challenging task. Conflicts of law, conflicts of interest, and conflicts of duty arise on a regular basis, bringing ever-deeper challenges for corporate IT teams and general counsel. These challenges emerge most crucially in responding to cross-border regulatory reviews, or cross-border litigation, both of which are events which company IT departments are generally not set up to deal with on a day-to-day basis. These are exceptional events, and they create exceptional challenges. For example, in February, Credit Suisse was before a US congressional committee regarding legacy tax evasion claims. Brady Dougan, CEO of the bank, said:

> *While Credit Suisse deeply regrets and takes responsibility for those violations, those actions should not overshadow the bank's ongoing commitment and consistent dedication to compliance with US law… We are fighting Swiss lawsuits trying to prevent our delivery of information to US authorities… Nonetheless, we fully intend to continue to press for our ability to co-operate with US authorities to the fullest extent allowed by law. These are not the actions of an institution flouting US law enforcement or hiding behind Swiss law.*

Corporations involved in cross-border investigations and litigation should always pay close attention to the way in which their data is collected, which data can or cannot be collected, and whether it can be transferred.

One further complication is the fundamental difference between civil and common law legal systems. Common law legal systems, such as the UK or the US, create obligations of data preservation and disclosure for parties involved or likely to be involved in civil or criminal litigation. Civil law legal systems, meanwhile, do not usually include such principles, and therefore when an enforcement agency or a litigant from a common law jurisdiction interacts with a company in the civil law world, conflict arises.

Often the first difficult challenge for the company in this situation is to quickly map out the obligations on the one side (eg, to provide data to an agency) with the restrictions of local civil law (eg, blocking statutes, data privacy, banking secrecy). In some cases, where regulatory action or litigation reaches into certain industries and territories, issues of national security may arise. It is also important to consider not just EU data protection rules, but also those that exist in other jurisdictions where, for example, previous dictatorial regimes have given rise to strict laws to protect individuals (eg, Argentina) as well as other jurisdictions where national security and sovereignty, and all the politics surrounding such, are the key drivers (eg, Russia and China).

The points below are important to consider in such circumstances:

Consider applicable jurisdictions and the related data privacy statutes.

Being a global company means working in multiple legal jurisdictions and potentially responding to investigations and data requests from two or more enforcement agencies with different requirements and goals. It is important to assess the countries touched by the investigation, note that data may be located in other jurisdictions, and assess the overlap or contradictions of their data privacy laws to ensure compliance with all and not select jurisdictions and related regulations. Avoid jurisdictional myopia.

Don't breach one law to comply with another before considering the risks and potential solutions.

The 2007 case of *Strauss v Credit Lyonnais* highlights the blatant differences between US and French data privacy law. The French counsel to the defendant ignored applicable procedures for transferring data during foreign legal proceedings and was criminally prosecuted for such violations. Two years prior, in the case of *Petroleos de Venezuela SA v Lynondell-Citgo Refining LP*, the counsel for the defendant corporation declined to produce documents to avoid violation of the Venezuelan blocking statute. The US court inferred that the evidence would have had an adverse effect on the defendant's case. However, the corporation and their legal counsel avoided the fines and potential imprisonment had they violated Venezuelan data privacy laws.

Engage with authorities.

Working with local data protection authorities and ministries would provide for the best alternative to treating the data. For example, one jurisdiction would accept the redaction of certain data points to allow for transport, while another may allow for restricted access via the internet while maintaining the data within the countries. All such alternatives would allow corporations to identify not only a legally compliant data-sharing approach, but also cost-effective manners for the collection, processing and transfer of such data. It will also provide for greater control of the data during the discovery and investigation process.

Compliance with data protection laws and discovery requests is a challenging task and the risk of non-compliance is not only monetary, but includes reputational damages and criminal repercussions. However, compliance is realistic and can be achieved within the confines of a budget that is commensurate with the risk.

Image: nabihariahi/iStock/Thinkstock

First published in **Global Investigations Review** Volume 1 Issue 2