Splinternet: Do Data Localisation Laws Threaten the Global Internet?

Andrew Fawcett - Partner - Digital & Data
a.fawcett@tamimi.com - Abu Dhabi

June – July 2017

However, in the wake of the Edward Snowden whistleblowing leaks that revealed mass foreign surveillance wiretaps of the Internet, a number of governments are considering implementing data localisation laws.

In practice, data localisation laws are highly likely to fragment the Internet resulting in inefficiencies and greater costs. Many recent technological advances may be affected or impeded by such laws.

What is Data Localisation?

Data localisation laws require that businesses that operate on the Internet, store and process data within the country where the businesses are located rather than servers overseas. Businesses that do not comply can be barred from doing business in that country or receive substantial fines.

Late last year the Russian's communication authority, the Roskomnadzor, blocked access to the LinkedIn website to comply with a Moscow City Court ruling that LinkedIn was in breach of Russian laws that require websites to store personal data of Russian citizens on servers in Russia. LinkedIn reportedly had argued that the laws should not apply as LinkedIn does not have a physical presence in Russia and that its activity is international and not specifically directed at Russia.

The common justification for data localisation is the assumption that placing data abroad jeopardises security and privacy. However, it does not necessarily follow that data localisation will actually prevent surveillance, as physical access is not technically necessary in order to conduct such activities. Furthermore, data localisation laws can be used as a means for governments to ensure that data is more readily available to their own domestic law enforcement.

In November 2013, Richard Salgado, Google's director of law information and information security is reported to have told a US congressional panel "If data localisation and other efforts are successful, then what we will face is the effective Balkanization of the Internet and the creation of a 'splinternet' broken up into smaller national and regional pieces, with barriers around each of the splintered Internets to replace the global Internet we know today."

Some consider that data localisation laws can be used by countries as a trade protection strategy used to provide local businesses with competitive advantage to increase their share of domestic IT markets otherwise dominated by global IT companies. The reality is that any economic gains will be likely limited to a few local sectors, such as data centres. Such gains are likely to be small compared to the potential harm done to the remainder of the digital economy.

Where are these Laws Being Introduced?

Data localisation laws already exist in various forms and degrees in several developed and developing countries.

Vietnam requires Internet service providers to maintain copies of data within Vietnam to allow for possible

government inspection. Australia prohibits the transfer of health data out of Australia in some situations. Indonesia requires companies to have data centres and disaster recovery centres the territory of Indonesia.

Arguably, although not strictly classed as a data localisation law, the EU's Data Protection Directive (and its successor, the General Data Protection Regulation), could be considered as effectively requiring data localisation because of the Directive's restrictions on transferring personal data to non-EU countries.

However, there is a newer more worrying trend emerging of more comprehensive data localisation laws with greater global reach. The previously mentioned law in Russia requires that any personal data of Russian citizens to be stored and processed within Russia. The law also requires the disclosure of the location of these data centres to the Russian authorities.

Recently the Cyberspace Administration of China called for public comments on its draft "Security Assessment for Personal Information and Important Data Transmitted Outside of China". These measures include a significant expansion of the data localisation measure that potentially applies to all businesses collecting data in China.

Some Developments in the GCC

A public consultation document issued in July 2016 by Saudi Arabia's Communications and Information Technology Commission ("CITC") called for comments on proposed Regulation for Cloud Computing.

The draft regulatory framework provides that "User Content" (defined as any data provided or generated under a contract for cloud services) will be subject to different levels of information security, depending on its sensitivity, origin, and other criteria.

It is proposed that no "Level 3" User Content can be transferred outside Saudi Arabia for whatever purpose and in whatever format, whether permanently or temporarily (e.g. for caching, redundancy or similar purposes).

While "Level 4" concerns highly sensitive or secret content belonging to concerned governmental agencies or institutions (and it is understandable that there may be a reason to localise such content), the "Level 3" classification in the proposed regulations is broader and includes "sensitive User Content of private sector companies or organisations". What is "sensitive" is not defined.

Cloud service providers are to presume that "Level 3" information security is to apply to any government authorities or agencies.

This proposed regulation can be contrasted with information security controls currently in place in the UAE. The National Electronic Security Authority ("NESA") has developed the 'UAE Information Assurance Standards' ("IAS") which include security controls for cloud computing. Compliance with the IAS is only mandatory for "UAE government entities and other entities identified as critical by NESA" (e.g. operators of critical IT infrastructure) – although NESA has recommended that all UAE entities who are not strictly subject to the IAS requirements should adopt them as a matter of best practice.

While the IAS does not prohibit cloud services, it does require an entity to define information security requirements covering the retention, processing and storing of data in cloud environments, which requires the consideration of regulatory and other requirements potentially limiting the processing, and storage of information in external entities for example, laws or business agreements preventing certain types of information from being stored outside national borders.

This approach of mandating only that an entity must expressly turn its mind to what data it is storing outside national borders and the security of that information in the context of what is best for its particular operations is preferable to having a blanket prohibition that requires data localisation. This appears to

provide more scope for balancing business and national interests.

Where Should Data be Stored?

If data localisation becomes commonplace, determining what data must be stored in which country may be easier said than done.

If Company X is headquartered in India but has subsidiaries around the world, does that mean that under data localisation laws all of Company X's data would have to be stored in India by the cloud service providers it uses to manage its online operations? Alternatively, should localised data be stored in the country of each Company X subsidiary? Will the country of incorporation matter or just the country where the relevant office or employee is located?

There are no clear answers as matters currently stand. Much will depend on how each jurisdiction drafts its data localisation laws on the issue.

What Does This Mean For Companies?

Data localisation laws create a significant barrier to companies seeking to expand their international presence. Widespread data localisation will require global service providers to build or rent physical infrastructure in each jurisdiction that requires data localisation. The associated costs and administration burdens will likely make the provision of many global services currently taken for granted by Internet users impractical.

Most markets in the GCC may be too small for many companies (e.g. start ups and app developers) to justify paying the costs associated with data localisation and consequently, a blanket imposition of data localisation by a GCC government means that the local markets risk getting left behind in the digital economy.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on legal issues to do with information security and data localisation. For further information please contact Andrew Fawcett (a.fawcett@tamimi.com) Nick O'Connell (n.oconnell@tamimi.com).