Digital Balkanisation: Is International Data Protection Going Global or Local?

30th April 2018

Digital Balkanisation:
Is International Data Protection Going Global or Local?

With just a month to go before the General Data Protection Regulation goes live on 25th May 2018, this report will study the implications for international data protection standards and we analyse whether the EU's impending regulation could help to drive a growing protectionist mentality. In our inter-connected era in which the U.S Congress has asked Facebook CEO Mark Zuckerberg to testify about his platform sharing information on 87 million of its users with Cambridge Analytica have we already entered a new period of data wars? Is data going global or going local? We also study potential threats posed to business resilience, national security and critical infrastructure in today's connected digital age.

Image: The Guardian

The headline connected risk of GDPR is that failure to comply by any company anywhere in the world that does business with Europe and holds personal data about EU residents – for purposes such as profiling and big data analysis – could result in fines of up to €20m or 4% of its global turnover, whichever is the greater. The risk of fines, however, is only the tip of data iceberg!

A survey published in November 2017 by cloud security firm HyTrust revealed as little as 22% of US organisations are concerned about the GDPR and have a plan in place. The survey included respondents from key industries, including government/military, financial/insurance, healthcare/biotech, manufacturing, transportation/shipping and technology.

More than half (51%) of respondents said their organisation is either not concerned about GDPR or is unaware of its relevance to their business. What is also interesting, however, are

the potential geo-political implications of the EU inspired regulation.

In theory, the EU regulator has the power to levy huge fines on U.S. (or other regions) businesses, healthcare providers, charities, individuals and other institutions that fail to comply. It will be interesting to see the reactions of the current U.S. Government administration if/when the fines land on the American desktops of corporate CEOs in 2018 or more likely 2019.

The UK's Information Commissioners Office says: "With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organisations, and to individuals. Having clear laws with safeguards in place is more important than ever given the growing digital economy."

According to an article in AdWeek: "A protectionist mind-set that has been brewing politically worldwide for quite some time is suddenly at the doorstep of every digital platform and global brand. Marketing players are now making locally-minded data moves that stand to hurt companies of all types; though the business ramifications have yet to be appropriately recognized."

"Certain governments already have data localization laws in place. Russia, for example, enforces data localization laws so that citizens' datasets have to remain in the country. Enforcing its laws, Russia has banned access to LinkedIn since 2016 and threatens to block Facebook in 2018 unless it agrees to comply with the data localization laws.

In Canada, British Columbia and Nova Scotia mandate that personal data held by certain public institutions must be stored and accessed within the borders of the country. There are 195 countries in the world. Imagine if software companies were required to have a service instance for every country—that scenario would likely drive their costs through the roof."

We are living in a period where Artificial Intelligence can deliver smart business tools and predictive data, in which the connected risk is that digital protectionism could hinder progress with negative impacts. One example that is cited if all data must be stored locally, then A.I. systems might draw only from data silos in each country, with the effect of creating seemingly nationally-biased "intelligence."

Fifth Step CEO and GDPR author Darren Way says: "Data is at the center of most businesses, GDPR will push more businesses to take a data centric approach to security and privacy. Some firms believe that it is an unachievable Nirvana to achieve a single control framework for cyber security and data protection globally, but there is a huge opportunity out there to achieve this right now."

We live in a world of global data flows but the regulatory response is fragmented and the definitions of personal data vary. A breakdown of key data regulatory in various territories follows:

USA Regulation

NYCR500 - All regulated entities and licensed persons of the Department of Financial Services (DFS) were required to file a cyber-security regulation Certification of Compliance under 23 NYCRR 500 by February 15, 2018

HIPPA - the Health Insurance Portability and Accountability Act, sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that all the required physical, network, and process security measures are in place and followed.

COPPA – The Children's Online Privacy Protection Rule imposes

certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

There are various requirements in these regulations for breach notification.

Canada Regulation

Canada's Anti-Spam Legislation (CASL) is a new anti-spam law that will apply to all electronic messages (i.e. email, texts) organizations send in connection with a "commercial activity." CASL is reportedly one of the toughest laws of its kind in the world, making its application and interpretation particularly thorny.

European Union Regulation

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all EU residents. When the GDPR takes effect, it will replace the 1995 Data Protection Directive (Directive 95/46/EC).

Russia Regulation

Russian Data Protection Act 2006 - Fundamental provisions of data protection law in Russia can be found in the Russian Constitution, international treaties and specific laws. All personal data operators are required to store and process any personal data of Russian individuals within databases located in Russia (subject to few exceptions). The penalty for violation of this requirement is ultimately the blocking of websites involving unlawful handling of Russian personal data.

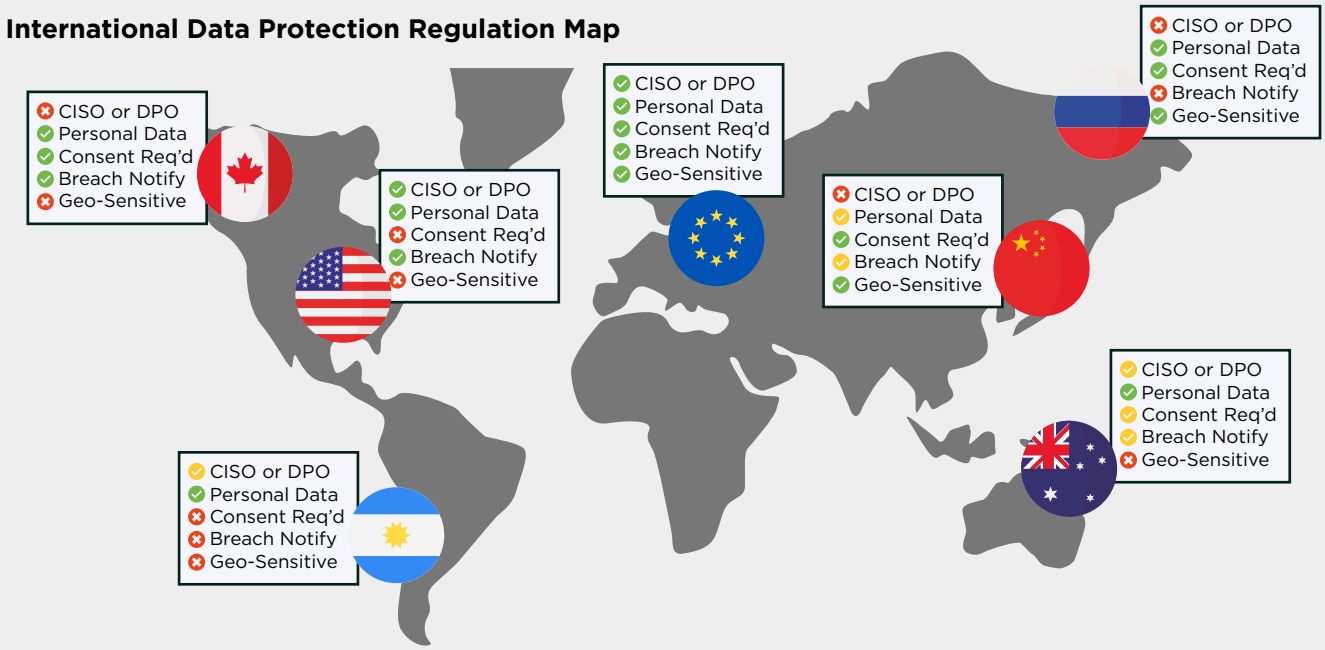
China Regulation

The Provisions on Telecommunication and Internet User Personal Information Protection - Until recently, China's data privacy framework has consisted of fragmented rules found in various laws, measures and sector-specific regulations. However, the Cyber Security Law (the CS Law), which came into effect on 1 June 2017, includes for the first time a comprehensive set of data protection provisions in the form of national-level legislation. These provisions are of general application to personal information collected over information networks.

Australia Regulation

Information Privacy Act 2014 - The Information Privacy Act commenced on 1 September 2014 and replaces the Privacy Act 1998. The Information Privacy Act 2014 (ACT)

International Data Protection Regulation Map



gives individuals greater control over the way that their personal information is handled. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Wray says: "A phrase that I seem to say a lot more frequently these days is: "You can outsource the function but can't outsource the responsibility." This doesn't just apply to GDPR, there are many governance or regulatory requirements that this applies to, so it worth remembering the phrase and making sure that it is a principle of your Vendor Management System, or your approach to any co-sourcing or outsourcing activity.

"The practical implications of this phrase is that you need to measure, monitor and manage the services provided by vendors, making sure that they are processing the data in accordance with applicable data protection regulation (GDPR in this case). Where they don't - and if there should be a violation or data breach - your organisation will be liable and you will be dealing your data protection authority to explain the nature, extent and mitigative actions that are being taken to pick up the pieces."

Next month GDPR goes into effect as part of the EU's attempt to catch up with technological advances that have exploded into millennial public consciousness. It is astonishing to think that when the previous EU data directive was adopted, both Google and Facebook were just twinkles in their parents eyes! GDPR has ultimately been created to protect EU residents' privacy from businesses in markets with less robust privacy protections, and in doing so will act as a catalyst to the rest of the world to conform to its standards.

Yet could GDPR be part of a wider picture of nationalist-based separatism that's been brewing for some time? AdWeek reports: "Before Brexit rocked the political-economic landscape in 2016 and GDPR was adopted the same year, there were already signs of digital protectionism in Europe. In 2014, German Chancellor Angela Merkel momentarily proposed the idea of the EU building its own Internet to prevent email and other data from flowing through U.S. networks. That move was a direct reaction to unflattering reports of data collection by the U.S. National Security Agency."

It has been widely reported how Equifax and Target suffered thanks to their own respective security breaches. Strava, a mobile fitness platform, also featured in the news after it divulged the existence of secret U.S. military bases when soldiers

logged their exercise routines on its app.

Nigel Cory, a trade policy analyst at the Information Technology and Innovation Foundation, said in the Privacy Adviser, "We're seeing a growing trend, as dozens of countries are enacting these kinds of barriers to data flows, targeting a growing range of data types, including personal data, but beyond that."

"Whether it's a splintering or Balkanization or whatever you call it," Cory said, "this presents a real risk to the global economy and innovation."

Some data experts anticipate consumer data wars between companies that customers trust enough to compile their personal data and the companies forced to let their data go. According to MITSLoan Management Review: "In this environment, the "haves" will be able to keep customizing and improving their offerings to EU citizens using more data than they ever dreamed accessible. At the other end of the spectrum, new products and services sold by "have-nots" will likely emerge slowly — or worse, miss the mark entirely because of the lack of insight into evolving customer needs and tastes."

In the new data landscape, firms will look to access data from rivals and companies with a footprint outside their vertical sector by tempting customers to transfer their data. They could do this by offering cheaper services to clients who choose to let these companies hold their personal data.

As the MIT article explains: "Traditional barriers to entry based on data collected over decades will be demolished, enabling small and nimble tech-based competitors that gain consumers' trust to become potentially widespread."

In this brave new connected data world, it will become common for companies to hire a data protection officer (or use a DPO service), which is stipulated under GDPR in certain circumstances anyway, to supervise procedures and processes that will proliferate as companies scramble to invest in new technology that "captures unambiguous consent for personal data use."

Meanwhile, the online campaign to affect the 2016 U.S. presidential election is just the start of a "dark future" where data will become weaponized by hostile states, unless regulators and consumers push back, says the author of a new book on how to fix the crisis of trust in Silicon Valley.

"There will be major international crises and probably wars built around data," Andrew Keen says. "There will be a hot data war at some point in the future."

According to The Globe and Mail, far from democratizing the web, sites such as Facebook and YouTube are undermining traditional media outlets, "cannibalizing revenues from professional content creators, and allowing anonymous trolls to post content unconstrained by professional standards that could manipulate public opinion and "reinvent" the truth."

In Mr Keen's vision of the war for the future: "the villains are China and Russia, which are using online platforms to create surveillance states that undermine trust between citizens and their government. The heroes are countries such as Estonia, which has created a digital ID system for its citizens – one that alerts them each time a government agency accesses their data."

In fact, E-Residency is a new digital nation for global citizens, powered by the Republic of Estonia, which is the first country to offer e-Residency, a government-issued digital ID available to anyone in the world. It's a fascinating concept and worthy of analysis in its own right raising the prospect of globally connected E-Citizens.

International data protection regulation such as GDPR could effectively become state actors' weapon of choice in curbing the power of big tech in today's connected world. However, the West's relative openness and transparency, the messy business of liberal

democracy and legal systems that are behind the digital technology curve, means they are ill-equipped to create the structures needed to protect their residents' data rights.

In the wake of the 2008 global crisis there were fears that an escalation of protectionist pressures could trigger high-intensity protectionism as a reaction to the crisis, however those fears failed to materialise in any significant form. The new question is whether the simmering pressure cooker of international data regulation will bring together a harmonious blend of flavours or blow the lid off global digitally connected trade.

Connect with Russell

Russell Group is a leading risk management software and service company that provides a truly integrated risk management platform for corporate risk managers and (re)insurance clients operating in an increasingly connected world.

Connected risk refers to the growth in companies which are increasingly integrating across industrial sectors and geographies, and creating greater levels of risk. This exposes corporates and (re)insurers to a broader range of inter-related perils, which requires a risk management approach built upon deep business intelligence and analytics.

Russell through its trusted ALPS solution enables clients whether they are risk managers or underwriters to quantify exposure, manage risk and deliver superior return on equity.

If you would like to learn more about Russell Group Limited and its risk management solutions, please contact rborg@russell.co.uk or visit www.russell.co.uk/contactus