DATA PROTECTION

Rachel Roumeliotis *explores the implications of living in an isolationist world and what it does to our data privacy*

We live in the age of data. We are constantly producing it, analysing it, figuring out how to store and protect it and, hopefully, using it to refine business practices and better understand the markets and customers we work with. However, surprisingly we seem to be blasé about our use of personal information in the modern world and are constantly sharing data freely with one and all with little regard to the possible consequences that may arise from doing so. There are more than 100-million Alexa devices in our homes, for instance, listening in to our conversations every day and we don't seem to realise the effects it could be having to our privacy and personal information.

Not only this, but our use of Gmail too is routinely used to pick up on conversational keywords to sell goods and services back to us. It is an attempt to anticipate and monetise our conversations that has become routine across so many apps. Many of us have accepted it as part and parcel of modern day living and do little to address it.

But data protection becomes even more complicated as the world becomes increasingly isolationist. Brexit is just one example of a tumultuous, global political landscape that could have impacts on the privacy and protection world, as well as the current global pandemic, which is affecting every aspect of our personal and professional lives.

Whether becoming more isolationist or trying to be more of a global player, how countries regulate data is up for constant debate. The tensions between the US in its stance on Chinese telecoms company Huawei and more recently with the video platform TikTok, are just a couple of examples of how global tensions can spill out and change relations between nations when it comes to data and privacy.

Data protection policies are fragmenting, leading to a patchwork quilt of data protection models across the world. The French independent regulatory body, the Commission Nationale de l'Informatique et des Libertés, has mapped the regulations and protections that apply to countries around the globe.

It shows how data in Europe, blanketed by the General Data Protection Regulations (GDPR), is heavily protected. According to GDPR, everyone responsible for using personal data has to follow strict rules called the 'data protection principles' and must make sure the information is used fairly, lawfully and transparently. GDPR lists specific rights for individuals that companies need to be able to comply with. This includes granting people easier access to the data a company holds about them, as well as the need for a company to get consent from those that they are collecting data about.

However, despite regulations being pertinent in Europe, in other areas of the globe, particularly Africa and large parts of Asia and South America, they are relatively unprotected in terms of data privacy laws and many don't see it as an issue.

This shouldn't be the case and becomes even more of a problem when data spans the globe. Companies run multi-national operations and operate IoT devices throughout the world. Today, almost everything is connected and 'smart', whether that be TVs, thermostats, security systems, smart… everything. It's very easy for data from a regulated jurisdiction to be misused in a region where such protections just don't exist.

Data is no longer just data. A perfect storm of protectionism and the advent of data as an internationally traded good requires business leaders and politicians to regard data as part of the supply chain. It should be subject to the same trade and regulatory patterns.

It's widely accepted that free markets stimulate growth and in the past decade an unregulated data environment increased world GDP by 10 percent ($7-trillion). The implementation of GDPR will put the brakes on the market and will reportedly cost the 27 nations of the EU more than $200-billion, equivalent to 1.3 percent of GDP, primarily due to lost productivity and research.

HEALTH AND FINANCE DATA ARE TARGETS FOR BAD ACTORS LOOKING TO TAKE ADVANTAGE

For many, this increasing sense of isolationism is hampering the global growth of data-centric businesses. Historically, the free data exchange has enabled the internet to work seamlessly and become a global trade route.

What we know is that the widespread adoption of personal computers, smartphones, the internet, e-commerce, smart devices and social media did not arrive with a parallel understanding of privacy fundamentals. Users and businesses need to know what to do to protect themselves, above all else. Essentially, the buck stops with businesses; they need to adjust and honour the responsibility they owe when they start compiling, analysing and/or selling user data. This is tricky, particularly when it comes to financial, health, e-commerce and social media as privacy and data protection can clash with an organisation's business strategy.

GDPR lists specific rights for individuals that companies need to be able to comply with

Businesses will all need to understand the concept of personally identifiable information, and why serious steps are needed to protect that type of information. They need to be aware of the different types of regulation and how it obligates organisations to behave. They also need to engage in dialogue with key stakeholders to understand expectations and learn about best practices that go with data provenance.

It is incumbent upon businesses, and the individuals that work for them, to equip themselves with enough knowledge to take appropriate data safety precautions and carefully consider the everyday trade-offs they make between convenience and how their data gets used. This is especially true in an isolationist world where data privacy regulations vary so enormously from one jurisdiction to another.

There are various ways individuals can improve their data privacy regime and ensure they remain as vigilant and secure as possible. These can include:

Making sure to check and adjust privacy settings in the privacy and security settings on browsers, social media apps and on mobile devices. That includes the device's operating system, wireless carrier extensions and the apps installed on the device.

Adjusting security settings on every smart device. If it's connected to the internet, users need to understand and adjust its privacy settings. Consider your wi-fi router the 'front door' to your smart home. Like any front door, it should be solid and equipped with strong locks to ensure cyber criminals can't access it.

Clearing cookies on a periodic basis, or even better, turning them off. It's always a good idea to clear out the cache or browser history and clear the cookies regularly. Your saved usernames and passwords will be deleted, but your privacy will be more secure and your browser will work better in the long term.

Paying attention to what the browser vendors provide in the way of privacy and security – keep in mind that when users log-in to applications, websites or services, then the browser, and potentially the browser vendor, know what they are doing.

Backing up important data with strong encryption or through cloud services that promise privacy, security and redundancy. The purpose behind online

backup is simple and straightforward: it protects your information, both business and personal, from the risk of loss associated with hacking and other technological disasters.

Paying particular attention to health and finance data – they are likely targets for organisations or bad actors looking to learn more about an organisation.

GDPR WILL REPORTEDLY COST THE 27 NATIONS OF THE EU MORE THAN $200-BILLION

Using appropriate passwords, two-factor authentication and password managers for common sense protection.

Unplugging when you can. The best way to protect privacy is not create data a company doesn't want to fall into the hands of others.

The may seem daunting, but don't despair. Investing a little time and common sense can bring peace of mind for those engaging in technology that surrounds us all. If in doubt, turn to Stay Safe online from the National Cyber Security Alliance for further guidance to navigate a safe path for data protection in the age of isolationism.

ROOM FOR IMPROVEMENT

Organisations should also take formal steps to condition and improve their data privacy. This will be an ongoing process and C-suite buy-in – although difficult to obtain – will be key to creating this long-term strategy. The C-suite, like many others in the organisation, will need education and understanding around the importance of this project, with a focus on the business benefits it will enable.

C-suite buy-in is also vital because data conditioning is not easy or cheap. Committing to formal processes, implementing technology and creating a dedicated team takes time and money. An ROI-based approach should help to determine what data conditioning is a priority and what is not worth addressing.

Data privacy might feel like a bit of an overwhelming problem. Just remember to start with the basics and encourage good data hygiene practices in your personal life and throughout your organisation. Technology and tools are great, but it all starts with people and how much of a priority they make their data ●

Rachel Roumeliotis - Vice President of Data and AI at O'Reilly – leads a team that covers a wide variety of programming topics, ranging from data and AI, to open source in the enterprise and emerging programming languages.

There are more than 100-million Alexa devices in homes across the world listening in to conversations