A Data Deficit:

The Risk of Getting it Wrong

The second of a three part series

Canadian Chamber of Commerce
Chambre de Commerce du Canada

The Voice of Canadian Business™
Le porte-parole des entreprises canadiennes^MD

This report was made possible by the generous support of our sponsors

Platinum

Microsoft

Gold

ALGONQUIN COLLEGE

ENBRIDGE

LoyaltyOne

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

Silver

Google

RBC

ROGERS

In 20 years, the internet has transformed from novelty to necessity. When Google was launched in 1998, at that time there were 2.4 million websites on the World Wide Web. There was just enough variety to capture the attention of the average person. Yet, only one in three people had a personal computer.[1] Few gave much thought to the volume of data that web traffic was generating and how valuable that data might be for solving problems, creating new products and services, and generating wealth.

Now the ratio of computer ownership is virtually one to one – everyone has some form of personal computing device. Today there are almost 2 billion websites (170 million active), serving up massive volumes of content to those personal computing devices.

The headlines for digital in 2018:

The number of internet users in 2018 is 4.021 billion, up 7% year-on-year
The number of social media users in 2018 is 3.196 billion, up 13% year-on-year
The number of mobile phone users in 2018 is 5.135 billion, up 4% year-on-year

The International Monetary Fund (IMF) notes the complexity in defining the digital economy and distinguishes between the economics of digital platforms and the digitalization of processes.[2] While estimations may vary depending on how narrowly the digital economy used is defined, some indicate the global internet economy stood at $1.55 trillion in 2017, with a target of $2.6 trillion by 2022.[3]

The data generated by all this activity is growing at a rapid pace. By 2020, the new information generated per second for every human being will approximately amount to 1.7 megabytes and the accumulated volume of big data will increase from 4.4 zettabytes to roughly 44 zettabytes – that's a mind boggling 44 trillion GB.[4]

It is within this context of growth, complexity and prosperity that we are now seeing the development of a global dialogue on how exactly this immensely high volume of data gets used and by whom.

As with any value proposition, success attracts predators. The nature of interconnected datasets leave room for misuse and abuse.

In this, our second segment examining Canada's data framework, we explore how many nations are reacting to the use and abuse of personal information through privacy legislation. Globally, 67% of nations have privacy laws or are currently drafting them. Most recently, some of the most significant changes to privacy laws occurred in Europe in May 2018, with the implementation of the General Data Protection Regulation (GDPR), which introduced new concepts such as data portability, transparency and breach notification requirements. Canada introduced new legislation, amending its private sector laws in 2014, with the breach notification provisions came into force November 2018. Australia and New Zealand also introduced similar amendments recently and now the US Senate has a draft bill that will hold CEOs accountable for the personal information collected by their companies.

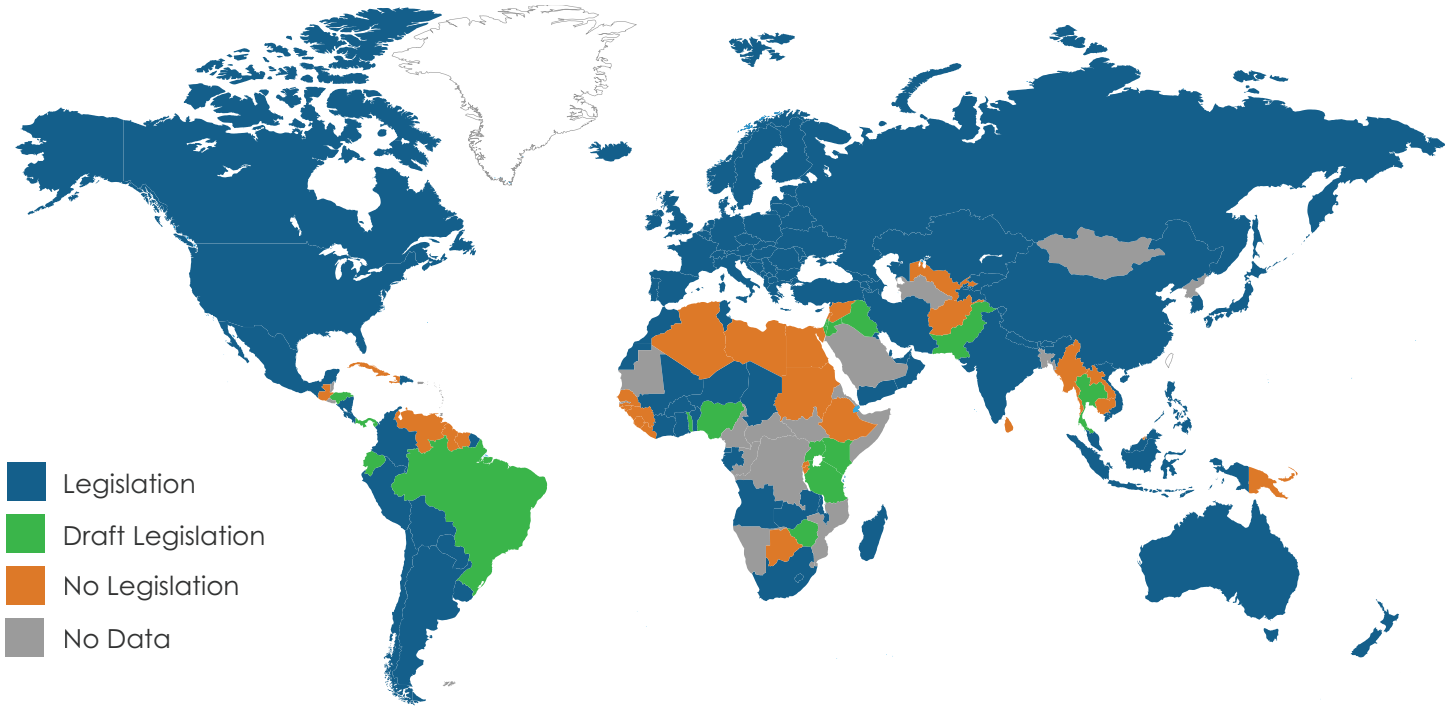
[1] http://www.nationmaster.com/country-info/stats/Media/Personal-computers/Per-capita#1998

[2] https://www.imf.org/~/media/Files/Publications/PP/2018/022818MeasuringDigitalEconomy.ashx

[3] eCommerce Report 2018: Statista Digital Market Outlook – Market Report

[4] https://www.newgenapps.com/blog/big-data-statistics-predictions-on-the-future-of-big-data

https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx



57% COUNTRIES WITH **LEGISLATION**

10% COUNTRIES WITH **DRAFT LEGISLATION**

21% COUNTRIES WITH **NO LEGISLATION**

12% COUNTRIES WITH **NO DATA**

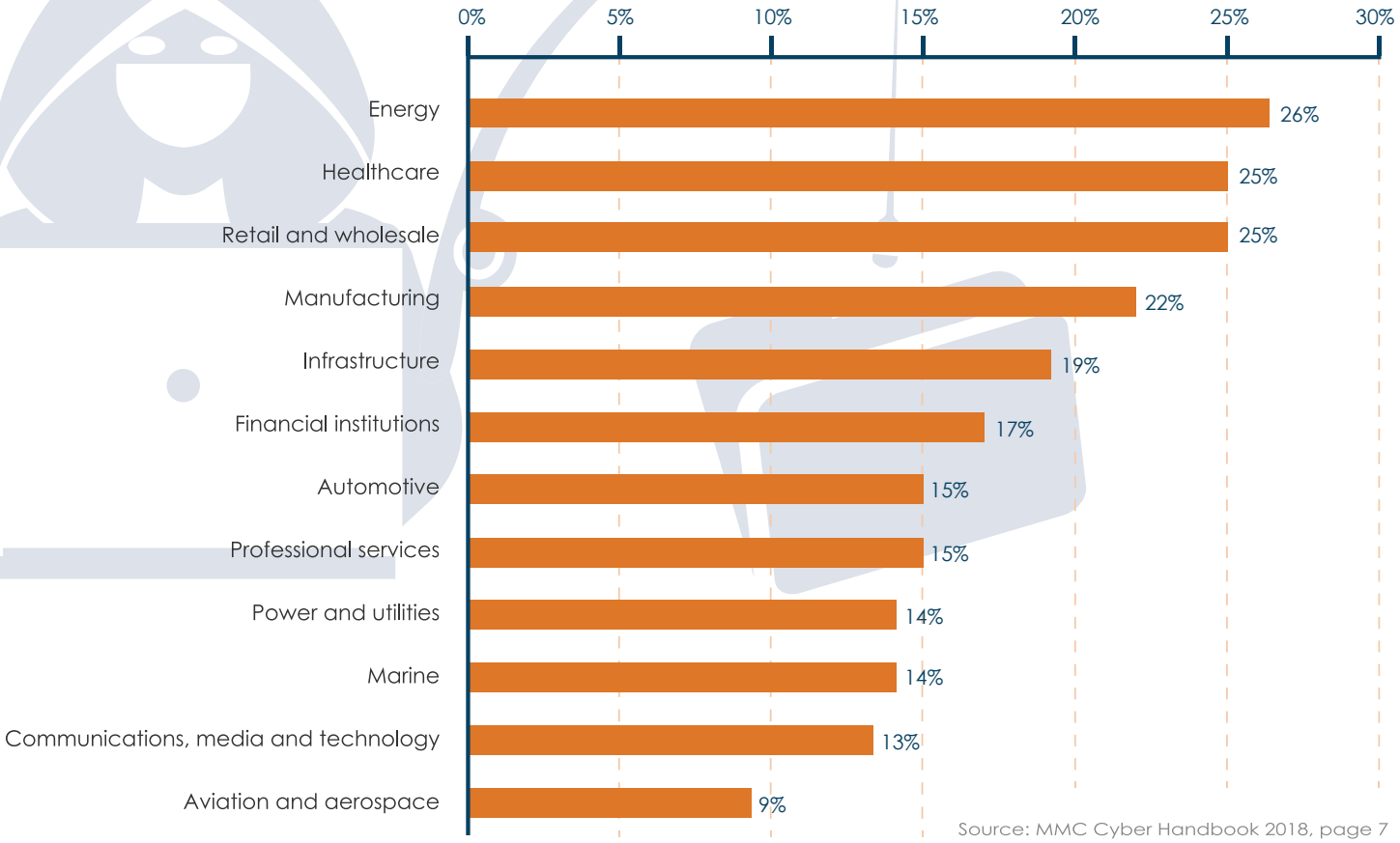
Taking the "we need more privacy" approach to addressing data breach phenomenon in the digital age, however, has unintended consequences for innovation and dismisses the notion that companies who have experienced a breach are themselves a victim. The costs managing a breach and subsequent regulatory oversight are reflected in higher downstream consumer prices.

Use, misuse and breaches

The data opportunity tends to be lost in the high profile public narrative around data breach and the misuse of data. For a multitude of valid reasons, companies and institutions keep extensive archival records on individuals. Some of the most sensitive data involve financial information and health data. Banks keep transaction records to meet the fiduciary obligations to banking customers and to meet regulatory compliance obligations. Pharmaceutical companies keep health care records of clinical trial participants to demonstrate the validity of new drug compounds.

Over the course of the last few years, we have seen an increasing number of security breaches with massive numbers of records compromised. These breaches have affected every industry, including health care, financial institutions and retail, affecting billions of people.

Industries impacted by cyber attacks worldwide as of September 2017



Source: MMC Cyber Handbook 2018, page 7

Financial loss, reputational damage, inconvenience and loss of trust for online transactions are just a few of the obvious negative impacts beaches can have on both the individual and the business. The below examples illustrate just how high and frequent these beaches can be, with almost four billion records having been compromised over the last five years.

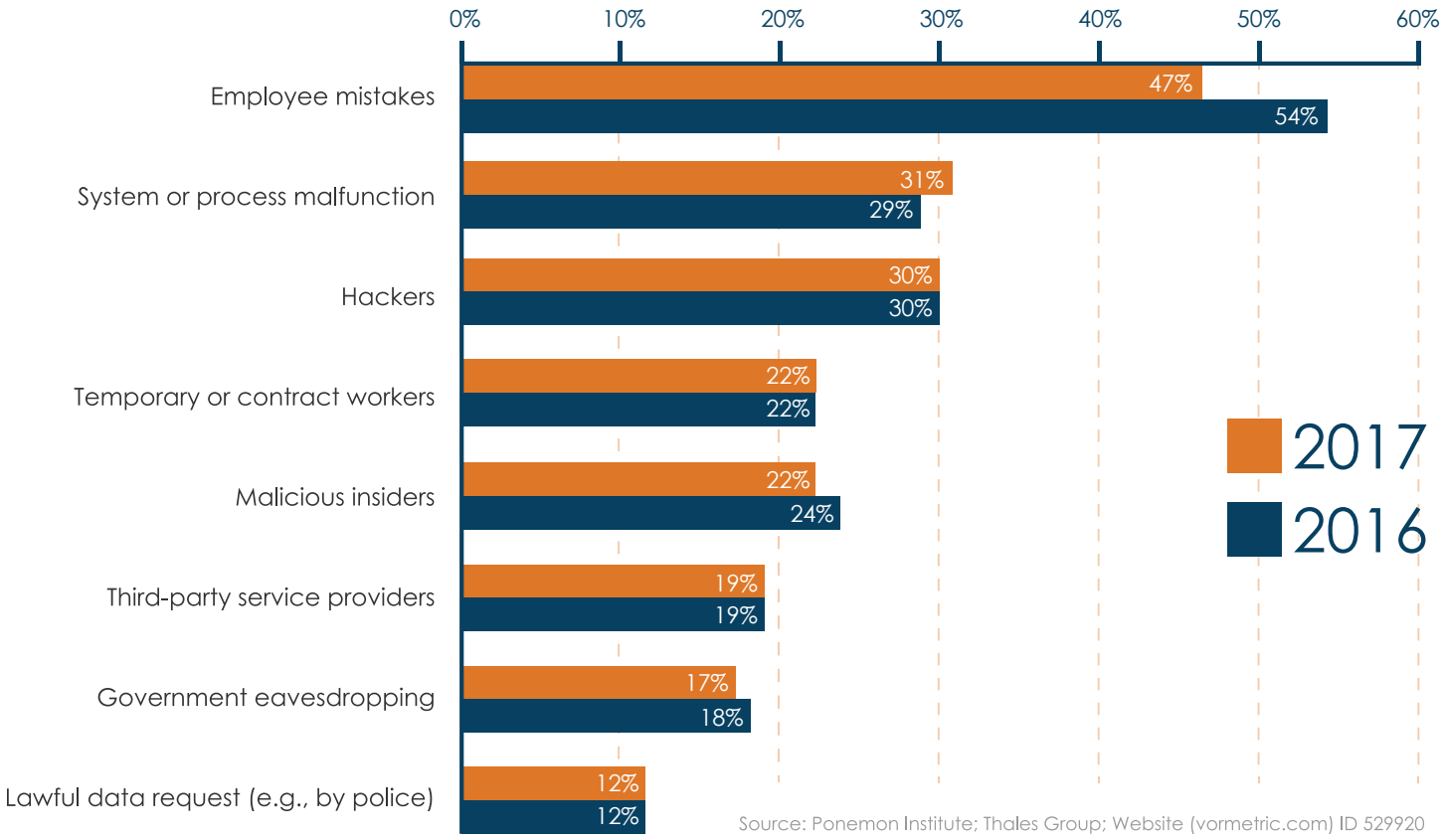
Company/Organization	Number of Record Stolen	Date of Breach
Yahoo	3 billion	Aug 2013
Equifax	145.5 million	Jul 2017
eBay	145 million	May 2014
Heartland Payment Systems	134 million	Mar 2008
Target	110 million	Dec 2013
TJX Companies	94 million	Dec 2006
JP Morgan & Chase	83 million (76M household, 7M small businesses)	Jul 2014
Uber	57 million	Nov 2017
U.S. Office of Personnel Management (OPM)	22 million	Between 2012-2014
Timehop	21 million	Jul 2018

Source: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101

For example, as a consumer credit reporting agency, Equifax Inc. collects and aggregates information on over 800 million individual consumers and more than 88 million businesses worldwide. Founded in 1899 and based in Atlanta, Georgia, it is one of the three largest credit agencies

In July 2017, a major cyber breach of Equifax affected over 143 million consumers in the U.S. The breach revealed the names, Social Security numbers, birth dates, and addresses of almost half of the total U.S. population.[5] Digital forensic analysis indicates that Equifax failed to patch a security program vulnerability and this has since become an example for businesses to improve their data handling, management and protection policies.[6]

Leading threats to sensitive or confidential data worldwide in FY2016 and FY2017



Source: Ponemon Institute; Thales Group; Website (vormetric.com) ID 529920

[5] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101

[6] https://www.trendmicro.com/vinfo/ph/security/news/cyber-attacks/equifax-reveals-extent-of-2017-data-breach-number-of-stolen-records

The very fact that a company widely used to monitor the credit of individuals who had been victims of previous cyber attacks, was itself attacked, has done significant damage to the public trust in online privacy. What must not be forgotten is the fact that in the case of a cyber breach, individuals are not the only victims. The businesses that suffer a cyber attack face revenue loss, property loss, reputational damage, and increasingly, administrative monetary penalties.

However, it is not just security breaches that have driven on the public discourse about data collection and privacy. Case in point: Facebook and Cambridge Analytica.

In 2014, Aleksandr Kogan allegedly took advantage of the tools and policies Facebook created for developers and used them to obtain information that was later transferred to the political-data firm Cambridge Analytica through an app known as Thisismydigitallife. The app was permissive and allowed developers to collect data not only on users who signed up for their app, but also on those users' Facebook friends. Facebook revised these policies in 2014, but this did not prevent Cambridge Analytica from allegedly engaging in a tactic referred to as "psychographic" targeting—advertising to people based on information about their attitudes, interests and personality traits.

The tactics used by Cambridge Anaytica shone a spotlight on the broader picture of data collection, data ownership and the rights of individuals. Fast forward to 2018, where many privacy setting defaults have now been adjusted on social media platforms in recognition of the consequences – market forces are adept at forcing change.

The Cambridge Analytica incident, while according to the available evidence does not involve non-U.S. user data, is also a centerpiece for government enquiry around the world and is frequently cited as a substantiation for adopting the prescriptive and punitive approach to the collection of personal data that is the model for the General Data Protection Regulation (GDPR) in Europe. While the reaction to stories like Cambridge Analytica and the move to introduce concepts like data localization, the right to be forgotten and data portability are understandable, these concepts have unintended consequences.

Unintended Consequences of the GDPR

In May 2018, the European Union brought into force a new privacy legislation regime that is intended to empower the individual to take back some control of the data collected about them. Some of the key features of the General Data Protection Regulation are:

1. **Transparency** – Information about personal data being collected and what it will be used for must be presented in clear, unambiguous language.

2. **Definitive Consent** – Permission to collect and used personal data must be obtained through "opt-in" mechanisms.

3. **Specific Permission** – Unless or until permission is granted by the individual to an app or website to use personal information in a specific way, it cannot be used for any other purpose or sell it to third parties.

4. **Privacy by Design** – Organizations may not request personal data that is not directly needed for the function of the app or software.

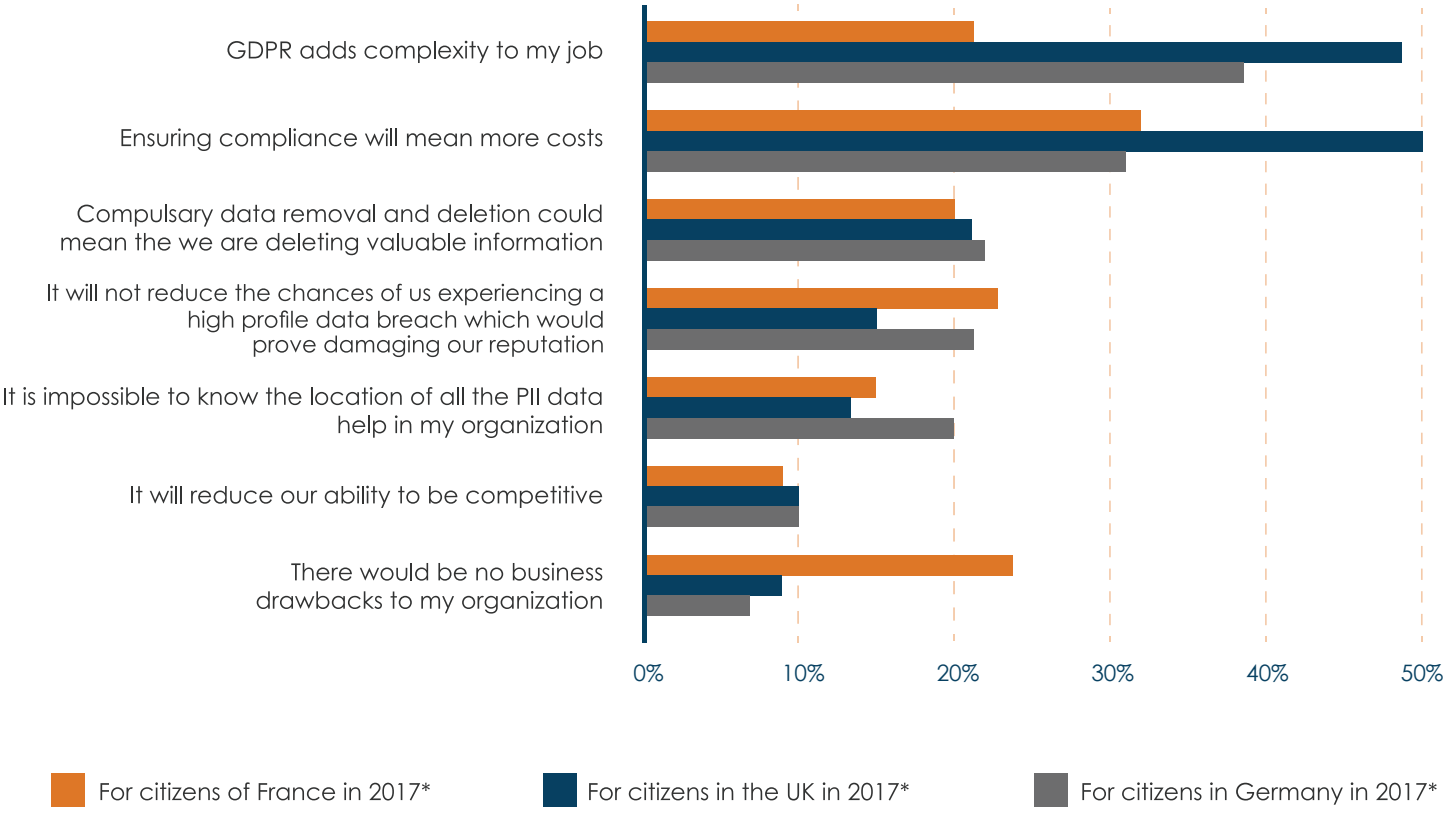
5. **Data Portability** – Individuals may request any data that a company has about them in a readable format so that it may be reused.

6. **The Right to be Forgotten** – Individuals may request that information that was publicly known at a certain time be deleted, that it be removed from search engine results and not allowing third parties to access the information.

7. **Data Localization** – The personal data of European citizens must be stored either in Europe or in a jurisdiction with substantially similar privacy legislation.

The move in Europe to re-envision the collection, storage, use and disclosure of personal information has numerous unintended consequences. The first is the impact of this new regime on the business model of ecommerce that has evolved over the course of 20 years.

Drawbacks of the EU GDPR for Organizations



There is a *quid pro quo* in the exchange of data for service. Consumers have come to expect the availability of "free" services. Search engines provide the service of linking people with relevant information. In exchange for the response to a search query, the individual pays the price of information submitted—IP address, location data, general interest, choice of search result explored. The search engine then uses this information to improve future search results and to drive revenues through advertising. The consequences of shifting to a pay-per-use system of launching queries would have a significant ripple effect through the internet economy.

The shift to an opt-in approach to consent for any collection of data will have two results: opt-in fatigue and a degradation of customer service.[7]

Pop-up screens (the scourge of '90's vintage internet sites) have returned in the form of requests for permission to use cookies. The business adage of "know your customer" will become more difficult in a regulatory environment that obligates data portability, reducing the ability of businesses to tailor services to a specific customer profile. There are no standards for how certain data sets are structured and interoperability becomes a problem in the transfer of a data set from one company to another. For example, in the made-to-measure apparel industry, measurement profiles are kept on file by retailers and are specific to a manufacturing model that may not be functional across all similar retailers in the industry. The default will be to delete the profile instead of transferring it, resulting in a frustrating customer experience and a lost innovation opportunity.

[7] Forbes, Aug 15, 2018

Consumers will also experience a reduction of variety of content. There are already examples of U.S.-based websites that have locked out European traffic because they are unable to comply with the GDPR. This is most distressing in the case of news outlets. The New York Times and the Chicago Tribune have closed their websites to European traffic for compliance fears, leaving European citizens with fewer options to stay informed.

The GDPR also has innovation implications. Technologies, such as block chain, that have the potential to build trust by securing and verifying transaction data, by their nature of copying data across thousands of computers cannot be GDPR compliant. The onerous nature of the compliance obligations makes it very difficult for smaller businesses that lack the resources of global companies to compete. It also makes it more difficult to track cyber criminals because the lack of footprints reduces the available forensic evidence.

As noted above, 67% of the world's countries have privacy legislation or draft legislation. A few, like Canada and Australia, now have mandatory breach notification regulations. While some have noted the ambiguity of obligations for determining significant harm can leave organizations vulnerable to sanctions, the granular and prescriptive nature of the regulations in the EU cause a significantly complex compliance burden.

Other countries, like Argentina and India, have right to be forgotten legislation. While the argument can clearly be made that an individual whose images were posted on the internet without his or her knowledge or consent should have a right to have those images deleted and deindexed, the argument to remove and deindex images that were posted with permission is more problematic. In Argentina, several lawsuits were launched to have images of celebrities deleted even though they were posted with permission. This has intellectual property and contract law implications.

With security breaches now commonplace, many nations are now considering data localization restrictions, where personal data must be stored within the physical geographic borders of the individual whose data has been collected. Canada, for example, has subnational (such as in British Columbia and Nova Scotia) legislation requiring data localization for the protection of health records. Perhaps this is the most poignant unintended consequence—the impact on healthcare. The technology now exists to undertake remote diagnostics and clinical care. For example, the medical device technology exists to treat patients with kidney disease in their own homes with portable dialysis machines, allo wing these patients to avoid weekly trips to major centres for treatment. However, the devices require the transfer of data across networks. Jurisdictions with the requirement of data localization of electronic health records can preclude patients from accessing this service, resulting in higher health care costs and increased inconvenience for patients.

While U.S. privacy law is still largely fragmented, there is a bill before the U.S. Senate that makes the GDPR seem like a light touch when it comes to limiting the ability of organizations to leverage big data. The Consumer Data Privacy Act, as the bill is tentatively named, has similarities to Europe's GDPR, which can fine companies up to 4% of their global, annual revenues for non-compliance. But the Consumer Data Privacy Act, introduced by Oregon Democratic Senator Ron Wyden, goes further by focusing on company CEOs. In addition to GDPR-style penalties, the proposed law would imprison executives up to 20 years, and individual fines could reach as high as $5 million for CEOs who knowingly mislead regulators.

The proposed law would require large organizations (revenues exceeding $1 billion or ones that store data on more than 50 million consumers or their devices) to submit annual data protection reports to the government that lay out their data-securing practices. It would force companies to comply with do–not-track policies while offering alternative payment options to consumers, such as subscription fees instead of ad-supported free models. And, it would boost the power of the Federal Trade Commission, adding a tech-focused division with a broader mandate alongside an arsenal of stronger enforcement actions.

While the internet connects the globe, privacy legislation globally is a patchwork. The EU is the first to enact legislation that has extra-territorial reach. The challenge facing Europe's trading partners is to find a balance in privacy legislation regimes that maintains the adequacy of substantially similar legislation without jeopardizing the ability to innovate with data. Some key considerations are:

- The need for improved methods to allow for international data transfers.
- The reduction of unnecessary administrative burdens.
- Increasing harmonization to create a predictable set of rules and expectations.

As noted by the co-chair of the International Chamber of Commerce task force on privacy and personal data protection, David Hoffman, "Enabling cross-border data flows is essential to further economic growth in today's information society. While promoting fundamental rights, the regulation should also eliminate unnecessary administrative burdens, such as removing bureaucratic hurdles to information flows." [8]

[8] https://cdn.iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf

Trust is Multifaceted

While it could be argued the fourth industrial revolution is already upon us, we are in its infancy. We still have time to get the regulatory framework right. Trust in the digital economy has been eroded by cyber breaches, the focus on function over security and the proliferation of nefarious actors spreading disinformation for self-interested purposes. Trust must be regained. However, trust in the digital economy encompasses many dimensions and the key components include: sound data governance, cybersecurity, intellectual property protection and privacy protection.

There need not be a trade-off between privacy and business innovation. New technologies can often better protect privacy. It would be short-sighted to think trust can be achieved only through regulation. Instead, user's knowledge of the environment, the associated risks and mitigation strategies they can, themselves, undertake as well as promotion of sound technology design all play critical roles in increasing trust in the digital economy.

The framework supporting how data is accessed, used and shared covers a broad spectrum of existing laws and programs (from privacy, competition, fraud, consumer protection, etc.) to self-regulation with industry-specific guidelines, technological solutions and education. A privacy policy is a key ingredient for the data economy, but pursuing it in isolation can undermine other important policy goals and considerations.

The right data strategy for Canada must clearly distinguish between sensitive personal data and the non-personal data of which the vast majority of data sets in the marketplace is comprised of. Most importantly, when considering adjustments to our regulatory framework, we must do so with an economic lens and not just a privacy lens. The application of this economic lens is best placed in the hands of an outside third party rather than the department or agency responsible for auctioning the regulatory adjustment.

In our third and final segment, we explore policy options that strike a balance between facilitating data innovation and respecting the privacy of the individual.

Canadian Chamber of Commerce | Chambre de Commerce du Canada